GFI LANguard 9.0 ReportPack

Manual

By GFI Software Ltd.

http://www.gfi.com
E-mail: info@gfi.com

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of GFI SOFTWARE Ltd.

Last updated: 4th September 2009

Version: LANSSRP-RP-EN-01.00.00

Contents

1. Introduction 1

1.1 About GFI ReportCenter 1
1.2 About the GFI LANguard 9.0 ReportPack 2
1.3 Components of the GFI LANguard 9.0 ReportPack 2
1.4 Key features 4

2. Installation 7

2.1 System requirements 7
2.2 Installation procedure 7
2.3 Launching the GFI LANguard reports for GFI ReportCenter 8
2.4 Selecting a product 8

3. Getting started: Default reports 9

3.1 Introduction 9
3.2 Generating a default report 9
3.3 Analyzing the generated report 13
3.4 Adding default reports to the list of favorite reports 14

4. Custom reports 15

4.1 Introduction 15
4.2 Creating a new custom report 15
4.3 Configuring data filter conditions 18
4.4 Run a custom report 23
4.5 Editing a custom report 23
4.6 Deleting a custom report 24
4.7 Adding custom reports to the list of favorite reports 24

5. Scheduling reports 25

5.1 Introduction 25
5.2 Scheduling a report 25
5.3 Configuring advanced settings 27
5.4 Viewing the list of scheduled reports 30
5.5 Viewing the scheduled reports activity 31
5.6 Enable/disable a scheduled report 32
5.7 Editing a scheduled report 32
5.8 Example: Scheduling a report 33

6. Configuring default options 39

6.1 Introduction 39
6.2 Configuring database source: Microsoft SQL Server 40
6.3 Configuring database source: Microsoft Access 41
6.4 Viewing the current database source settings 42
6.5 Configuring default scheduling settings 42
6.6 Importing/Exporting the configuration 43

7. General options 48

7.1 Viewing the product ReportPack version details 48
7.2 Checking the web for newer builds 48

8. Appendix: GFI LANguard default reports 50

8.1 Vulnerability assessment reports 50
8.2 Network and software audit reports 65
8.3 Results comparison 81

9. Troubleshooting 85

9.1 Introduction 85
9.2 Knowledge Base 85
9.3 Web Forum 85
9.4 Request technical support 85
9.5 Build notifications 86

Index 87

1. Introduction

1.1 About GFI ReportCenter

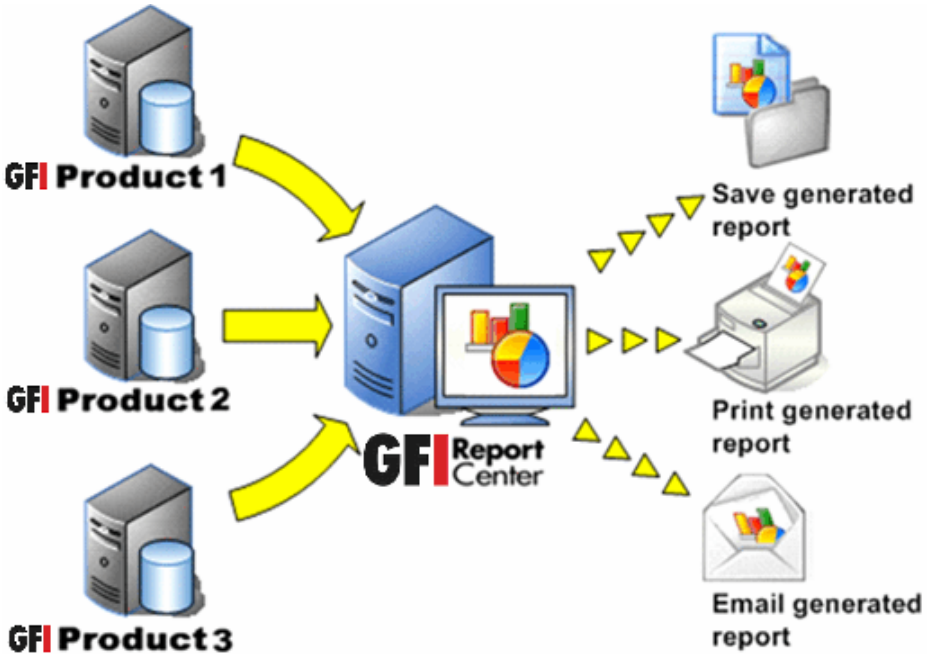


Figure 1 - Centralized reporting framework

GFI ReportCenter is a centralized reporting framework that allows you to generate various reports using data collected by different GFI products. GFI releases specialized reports for each of its products, referred to as a ReportPack; for example, the GFI LANguard ReportPack. A ReportPack can be downloaded as an add-on to the GFI product.

Figure 2 – Several Report Packs plugged into the GFI Report Center framework

A ReportPack plugs into the GFI Report Center framework; allowing you to generate, analyze, export and print the information generated through these reports.

1.2 About the GFI LANguard 9.0 ReportPack

The GFI LANguard ReportPack is a full-fledged reporting companion to GFI LANguard (GFI LANguard). It allows you to generate graphical IT-level, technical and management reports based on the network security audits carried out by GFI LANguard

From trend reports for management (ROI) to daily drill-down reports for technical staff; the GFI LANguard ReportPack provides you with the easy-to-view information required, to fully identify any vulnerability on your corporate network.

The GFI LANguard ReportPack allows for the creation of various graphical and text based reports related to:

- Vulnerability assessment reports
- Network and software auditing reports
- Results comparison reports.

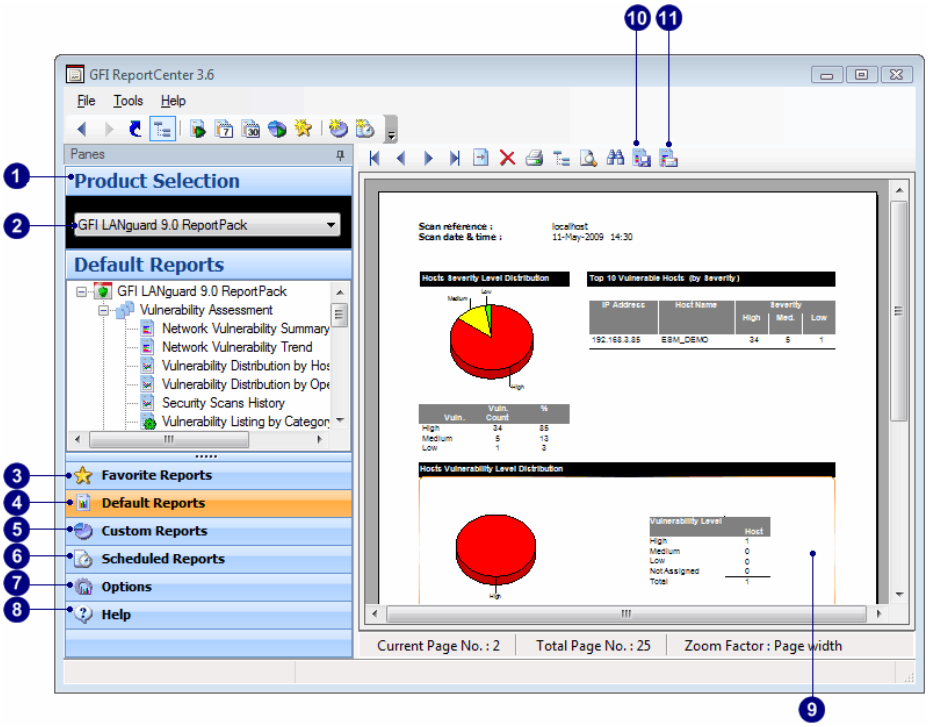
1.3 Components of the GFI LANguard 9.0 ReportPack

When you install the GFI LANguard 9.0 ReportPack, the following components are installed:

- GFI Report Center framework
- GFI LANguard 9.0 default reports
- Report scheduling service.

GFI Report Center framework

The GFI Report Center framework is the management console through which you can generate the specialized product reports which are shipped with a product ReportPack. The GFI Report Center framework offers a common application interface through which you can navigate, generate, customize and schedule reports.



Screenshot 1 – The GFI ReportCenter management console

The GFI ReportCenter management console is organized as follows:

1	**Navigation Pane** – Use this pane to access the navigation buttons/configuration options provided with GFI ReportCenter.
2	**Product Selection drop-down list** – Use this drop-down list to select the GFI product for which to generate reports. The Product Selection drop-down list displays all the products for which you have installed a ReportPack.
3	**Favorite Reports** – Use this navigation button to access your favorite/most used reports. For more information on how to add reports to this list refer to the 'Adding default reports to the list of favorite reports' and 'Adding custom reports to the list of favorite reports' sections in this manual.
4	**Default Reports** – Use this navigation button to access the default list of reports which can be generated for the selected product. For more information on default reports refer to the 'GFI LANguard default reports' section in this manual.
5	**Custom Reports** – Use this navigation button to access the list of customized reports which can be generated for the selected product. For more information on how to create custom reports refer to the 'Custom reports' chapter in this manual.
6	**Scheduled Reports** – Use this navigation button to access the list of scheduled reports for automatic generation and distribution. For more information on how to create scheduled reports refer to the 'Scheduling reports' chapter in this manual.
7	**Options** – Use this navigation button to access the general configuration settings for the GFI product selected in the Product Selection drop down list.

8	**Help** – Use this navigation button to show this Quick Reference Guide in the Report Pane of the GFI ReportCenter management console.
9	**Report Pane** - Use this multi-functional pane to: View and analyze generated reports Maintain the scheduled reports list Explore samples and descriptions of default reports.
10	**Export** – Use this button to export generated reports to various formats including HTML, Adobe Acrobat (PDF), Excel (XLS), Word (DOC), and Rich Text Format (RTF).
11	**Send email** – Use this button to instantly distribute the last generated report via email.

GFI LANguard 9.0 default reports

The GFI LANguard 9.0 default reports are a collection of specialized pre-configured reports which plug into the GFI ReportCenter framework. These reports present the results of network security scans performed by GFI LANguard and allow for the generation of both graphical and tabular IT-Level, technical and management reports. Default reports can also serve as the base template for the creation of customized reports which fit specific network-reporting requirements.

Report scheduling service

The report scheduling service controls the scheduling and automatic distribution of reports by email. Reports generated by this service can also be saved to a specific hard disk location in a variety of formats which include DOC, PDF, RTF and HTML.

1.4 Key features

Centralized reporting

GFI ReportCenter is a one-stop, centralized reporting framework which enables the generation and customization of graphical and tabular reports for a wide array of GFI products.

Wizard assisted configuration

Wizards are provided to assist you in the configuration, scheduling and customization of reports.

Report scheduling

With GFI ReportCenter you can schedule reports to be generated on a pre-defined schedule as well as at specified intervals. For example, you can schedule lengthy reports to be generated after office hours. This allows you to maximize the availability of your system resources during working hours and avoid any possible disruptions to workflow.

Distribution of reports via email

GFI ReportCenter allows you to automatically distribute generated reports via email. In scheduled reports, this can be achieved automatically after the successful generation of a scheduled report.

Report export to various formats

By default, GFI ReportCenter allows you to export reports to various formats. Supported formats include HTML, PDF, XLS, DOC and RTF. When scheduling reports, you can optionally configure the preferred report output format. Different scheduled reports can also be configured to output generated reports to different file formats.

Default reports

The GFI LANguard ReportPack ships with a default set of graphical and tabular reports. These reports can be generated without any further configuration effort immediately after the installation. The default reports in this ReportPack are organized into three different report-type categories:

- Vulnerability assessment reports
- Network and software auditing reports
- Results comparison reports.

Report customization

The default reports that ship with every ReportPack can serve as the base template for the creation of customized reports. Report customization is achieved by building up custom data filters which will analyze the data source and filter the information that matches specific criteria. In this way, you create reports tailored to your reporting requirements.

Favorites

GFI ReportCenter allows you to create bookmarks to your most frequently used reports – both default and custom.

Printing

By default, all reports generated by GFI ReportCenter are printer friendly and can be printed through the windows printing services provided by the system where GFI ReportCenter is installed.

2. Installation

2.1 System requirements

Install the GFI LANguard ReportPack on a computer that meets the following requirements:

- Windows 2000 (SP4), XP (SP2/SP3), 2003, 2008, VISTA (SP1), operating system.
- Internet Explorer 5.1 or higher
- .NET Framework version 2.0
- MDAC 2.8
- GFI ReportCenter 3.6

NOTE: The GFI LANguard ReportPack only allows you to generate reports for data contained in scan results databases which were created and maintained by GFI LANguard

2.2 Installation procedure

The GFI LANguard ReportPack includes an installation wizard which will assist you through the installation process. During the installation process this wizard will:

- Verify that you are running the latest version of the GFI ReportCenter framework; if you are installing the framework for the first time or the currently installed framework version is outdated, the installation wizard will automatically download the latest one for you.
- Automatically install all the required components distributed including the GFI ReportCenter framework, the GFI LANguard default reports and the Report Scheduling service.

To start the installation:

1. Double-click **LANguard9rp.exe**.

2. Select the required language.

3. Setup will next list all the missing prerequisites (if any). Install any missing prerequisites by selecting the prerequisite and choosing **Next.**

NOTE: If the current version of your GFI ReportCenter framework is not compatible with the GFI LANguard ReportPack, you will be prompted to download and install an updated version.

4. From the welcome screen, click **Next**.

5. Read the End User License Agreement, check the **I accept the license agreement** radio button and click **Next.**

6. If prompted enter your registration details and license key. Click **Next** to continue setup.

NOTE: If GFI LANguard is already installed, GFI ReportPack automatically registers the license key of GFI LANguard.

7. Select installation path or leave it as default and click **Next.**

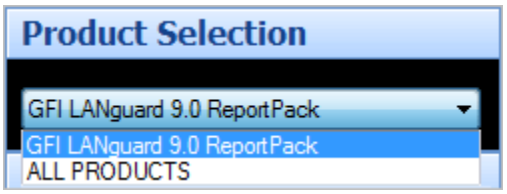
8. Select **Launch GFI LANguard 9.0 ReportPack** to launch ReportPack on setup completion.

2.3 Launching the GFI LANguard reports for GFI ReportCenter

Following the installation, launch the GFI LANguard Reports for GFI ReportCenter from **Start ► Programs ► GFI ReportCenter ► GFI LANguard 9 ReportPack.**

2.4 Selecting a product

When more than one product ReportPack is installed, use the **Product Selection** drop down list to select the GFI product ReportPack to be used.



Screenshot 2 – Product Selection drop down list

For example, to run the reports provided in the GFI LANguard ReportPack:

1. Launch GFI ReportCenter from **Start ► Program Files ► GFI ReportCenter.**

2. Select GFI LANguard 9.0 from the **Product Selection** drop down list.

NOTE: Select the **ALL PRODUCTS** option to display and navigate all the ReportPacks that are currently installed in GFI ReportCenter.

3. Getting started: Default reports

3.1 Introduction

After installing the GFI LANguard ReportPack, a number of specialized pre-configured reports can immediately be generated on the data stored in the database backend of GFI LANguard These default reports are organized into the following categories:

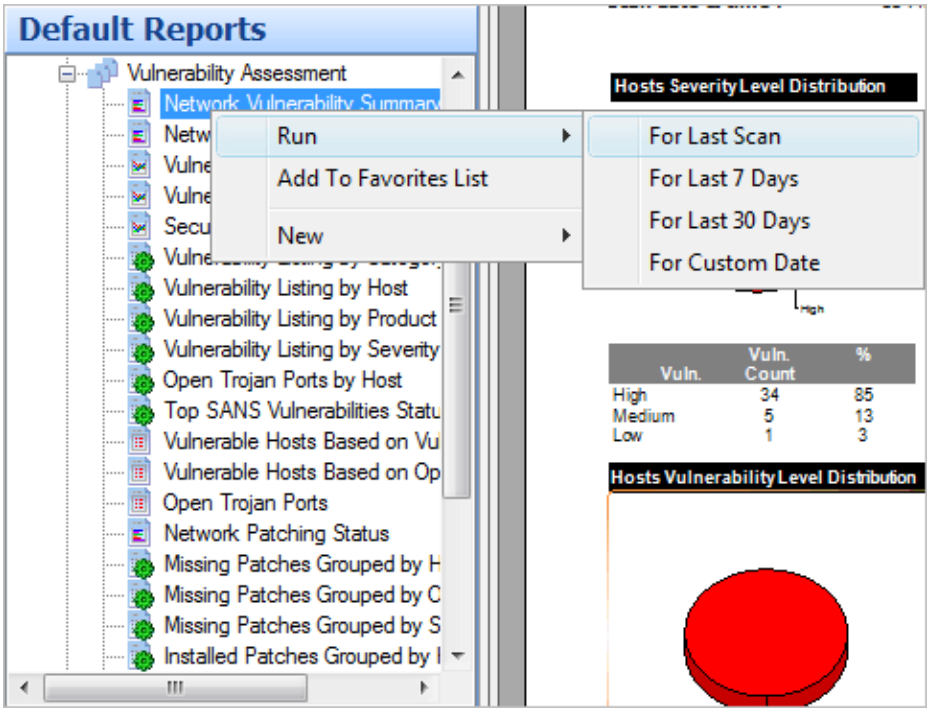
- **Vulnerabilities Assessment reports:** Use the reports in this category to identify vulnerabilities detected on the network as well information on network patches and service packs installed or awaiting deployment The reports include vulnerability details such as host machines, operating systems affected and severity.
- **Network and software audit reports:** Use the reports in this category to display detailed information on hardware and software present on the network. These reports help management in analyzing conformance with corporate security policy.
- **Results comparison reports:** Use the reports in this category to compare results of consecutive network scans that have a common profile and target, and of computer scans against a computer used as benchmark.

GFI LANguard default reports are accessed by clicking on the **Default Reports** navigation button provided in the navigation pane.

3.2 Generating a default report

To generate a default report:

1. Click on the **Default Reports** navigation button to bring up the list of default reports available.



Screenshot 3 – Selecting the data set

2. Right-click on the report to be generated, select **Run** and specify the scan date/time period that will be covered by the report.

Example 1: Generating a "Network Vulnerability Summary" report based on the last scan.

This example demonstrates how to generate a network vulnerability summary report based on the last network security scan carried out:

1. Click on the **Default Reports** navigation button to bring up the list of available reports.

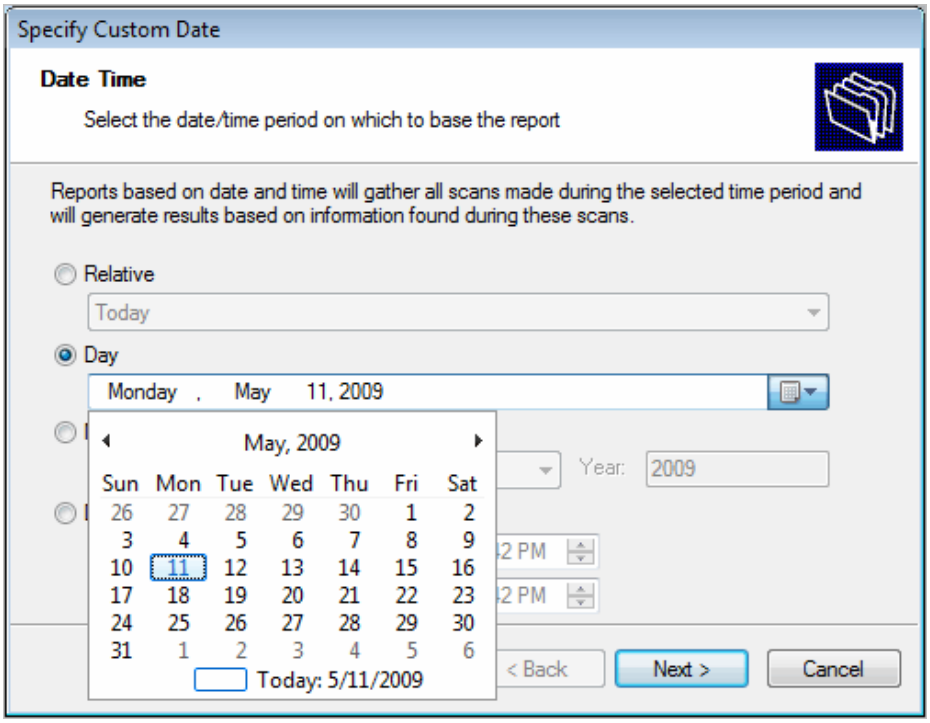
2. Right-click on **Network Vulnerability Summary** and select **Run ► For Last Scan**.

Example 2: Generating a "Network Vulnerability Summary" report based on scans made on a particular day.

This example demonstrates how to generate a network vulnerability summary report based on the scan performed on May 11, 2009.

1. Click on the **Default Reports** navigation button to bring up the list of available reports.

2. Right-click on **Network Vulnerability Summary** and select **Run ► For Custom Date**.


Specify Custom Date
Date Time
Select the date/time period on which to base the report
Reports based on date and time will gather all scans made during the selected time period and will generate results based on information found during these scans.
Relative
Today
Day
Monday , May 11, 2009
May, 2009
Sun Mon Tue Wed Thu Fri Sat
26 27 28 29 30 1 2
3 4 5 6 7 8 9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
31 1 2 3 4 5 6
Today: 5/11/2009
Year: 2009
2 PM
2 PM
< Back
Next >
Cancel

Screenshot 4 - Configuring custom date/time period

3. Select the **Day** option and expand the provided drop down. This will bring up the date selection calendar.

4. Navigate to the required month (i.e. May) and select the required day (i.e. 11).

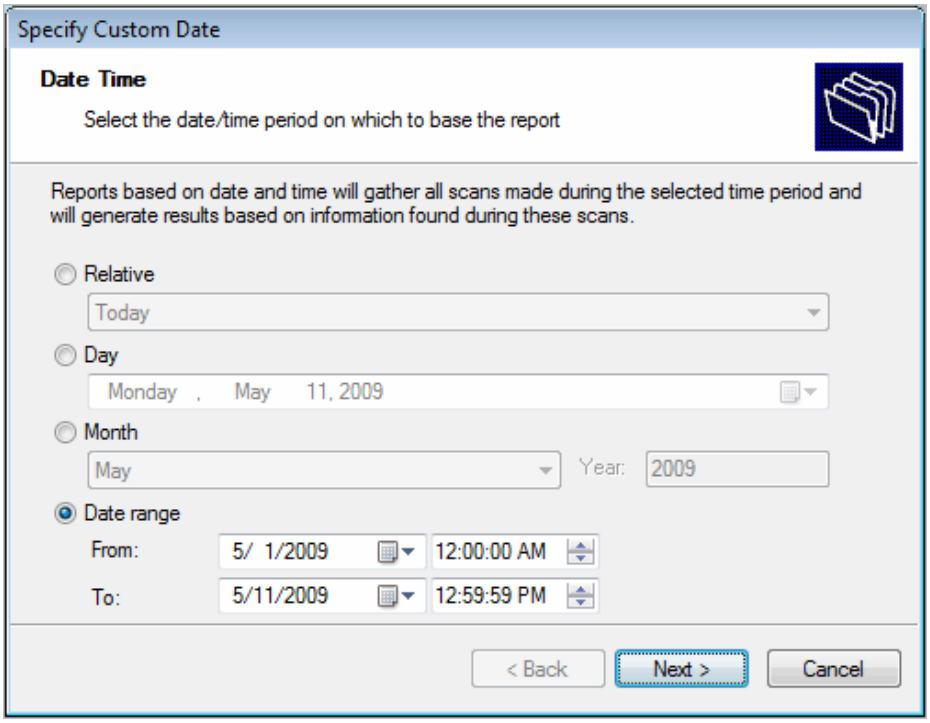
5. Click **Next** to generate the report.

Example 3: Generating a "Network Vulnerability Summary" report based on data collected over a specific date/time period.

This example demonstrates how to generate a network vulnerability summary report based on network security scans carried out between May 1, 2009 and May 11, 2009.

1. Click on the **Default Reports** navigation button to bring up the list of available reports.

2. Right-click on **Network Vulnerability Summary** and select **Run ► For Custom Date**.


Specify Custom Date
Date Time
Select the date/time period on which to base the report
Reports based on date and time will gather all scans made during the selected time period and will generate results based on information found during these scans.
Relative
Today
Day
Monday , May 11, 2009
Month
May
Year: 2009
Date range
From: 5/ 1/2009 12:00:00 AM
To: 5/11/2009 12:59:59 PM
< Back
Next >
Cancel

Screenshot 5 - Configuring custom date/time period

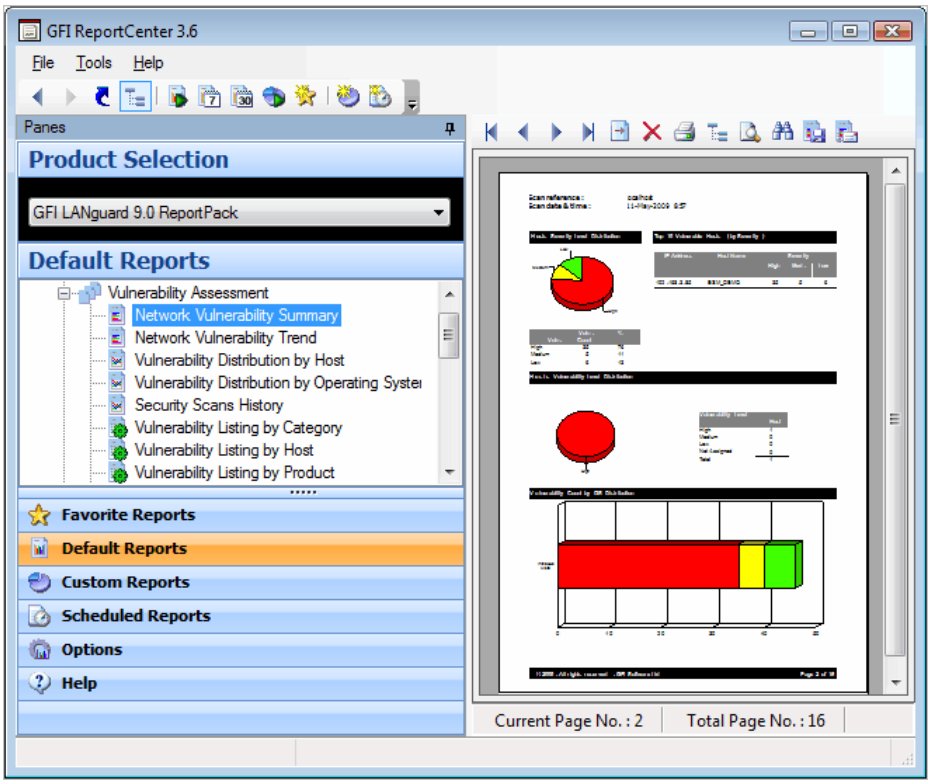
3. Select the 'Date range' option and specify the required parameters:

- 'From' – 5/1/2009 12:00:00 AM.
- 'To' – 5/11/2009 12:59:59 PM.

NOTE: Date and time format are based on the regional settings configured on your computer.

4. Click **Next** to generate the report.

3.3 Analyzing the generated report



Screenshot 6 – Generated reports are displayed in the right pane of the management console

Generated reports are shown in the right pane of the GFI ReportCenter. Use the toolbar at the top of the report pane to access common report related functions:

Report browsing options

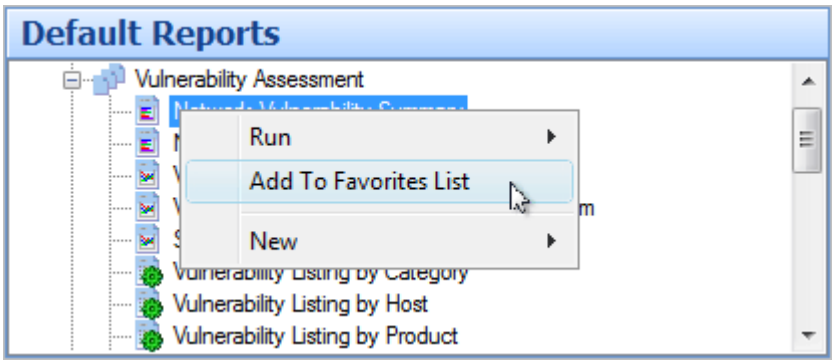
	Browse the generated report page by page.
	Zoom in/Zoom out.
	Search the report for particular text or characters.
	Go directly to a specific page.
	Breakdown the report into a group tree (e.g. by date/time).
	Print report.

Report storage and distribution options

	Export the generated report to a specific file format.
	Distribute the generated report via email.

NOTE: For information on how to configure report storage and distribution options refer to the 'Configuring Advanced Settings' section in this manual.

3.4 Adding default reports to the list of favorite reports



Screenshot 7 – Favorite Reports navigation button

You can group and access frequently used reports through the **Favorite Reports** navigation button. To add a default report to the list of favorite reports:

1. Click on the **Default Reports** navigation button to bring up the list of available reports.

2. Right-click on the default report that you to be added to favorites and select **Add to favorites list**.

3. Click **Yes** to confirm.

4. Custom reports

4.1 Introduction

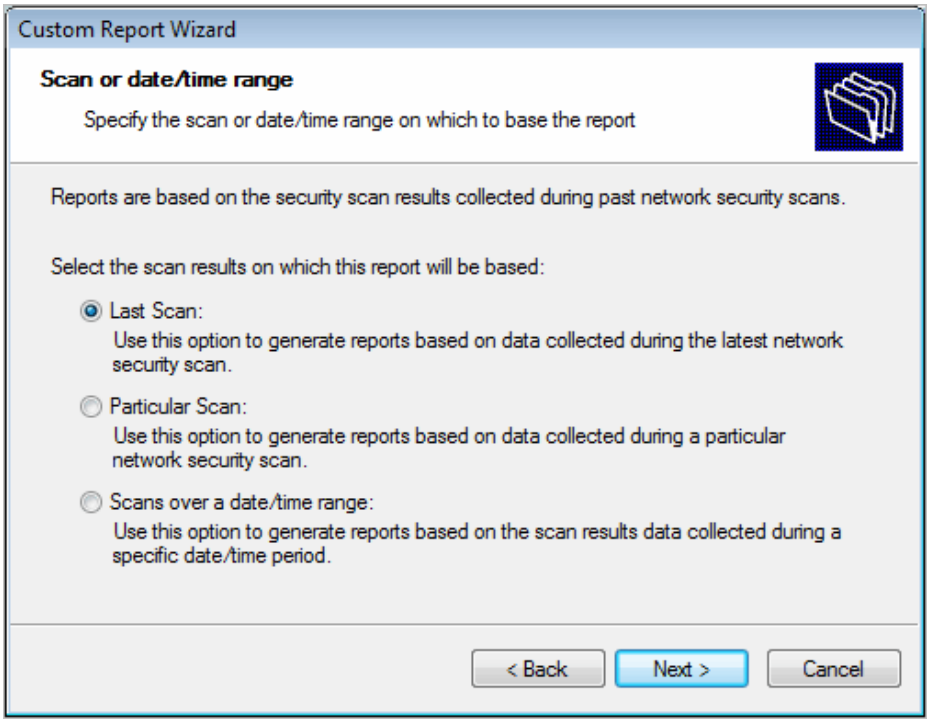
GFI ReportCenter allows you to create custom reports which are tailored to your reporting requirements. This is achieved by building up custom data filters which will analyze the data source and filter out the information that matches the specified criteria.

4.2 Creating a new custom report

To create a custom report:

1. Click on the **Default Reports** navigation button.

2. Right-click on the default report to be used as template and select **New ► Custom Report**. This will bring up the 'Custom Report Wizard'.

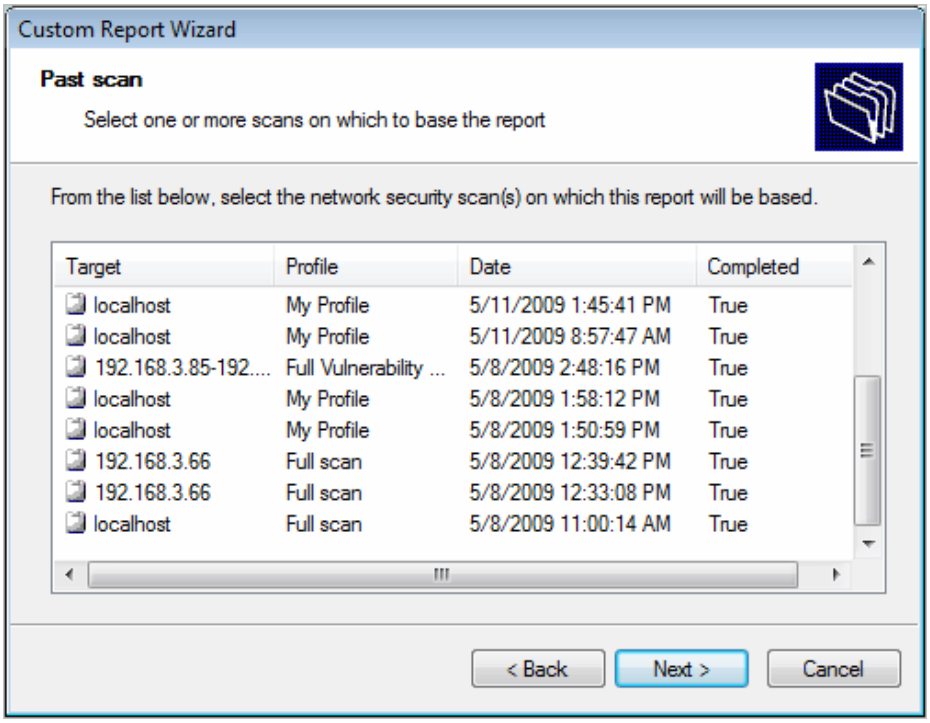

Custom Report Wizard
Scan or date/time range
Specify the scan or date/time range on which to base the report
Reports are based on the security scan results collected during past network security scans.
Select the scan results on which this report will be based:
Last Scan:
Use this option to generate reports based on data collected during the latest network security scan.
Particular Scan:
Use this option to generate reports based on data collected during a particular network security scan.
Scans over a date/time range:
Use this option to generate reports based on the scan results data collected during a specific date/time period.
< Back
Next >
Cancel

Screenshot 8 - Selecting the scan data source to use

3. Specify the data source option that will be used to generate the custom report. This data source refers to scan results from:

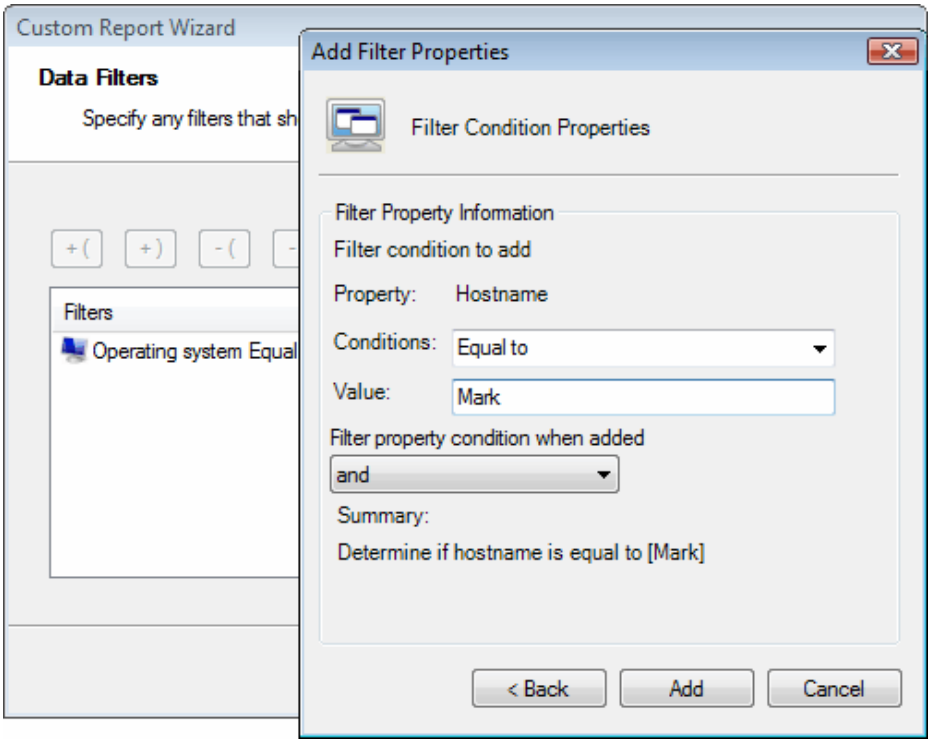
- the last scan
- particular scan(s)
- scans carried out over a specific date/time period.

Click **Next** to continue.



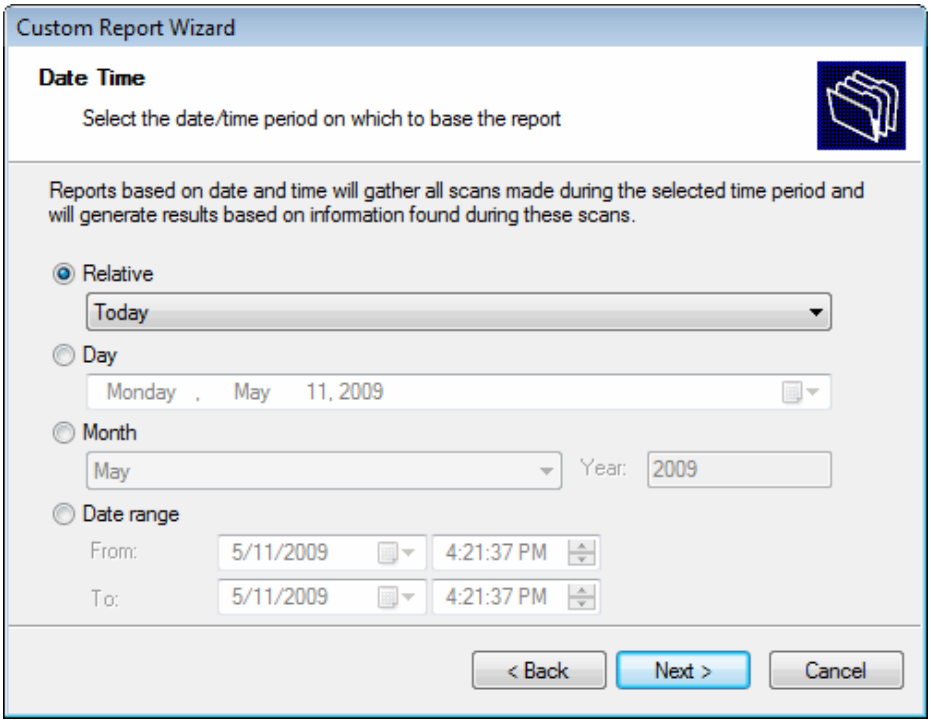
Screenshot 9 – Selecting the scan data source to use

4. If using the **Particular Scan** option, select the required scan(s) from the list of network security scans carried out on the corporate network. Click **Next** to continue.



Screenshot 10 – Specifying data filter conditions

5. Configure the data filter conditions that will be applied against the selected data source. Click **Next** to continue.


Custom Report Wizard
Date Time
Select the date/time period on which to base the report
Reports based on date and time will gather all scans made during the selected time period and will generate results based on information found during these scans.
Relative
Today
Day
Monday , May 11, 2009
Month
May
Year: 2009
Date range
From: 5/11/2009 4:21:37 PM
To: 5/11/2009 4:21:37 PM
< Back
Next >
Cancel

Screenshot 11 - Configuring custom date/time period

6. If using the **Scans over a date/time range** option, select the date/time period from which network security scan results will be gathered. Click **Next** to continue.

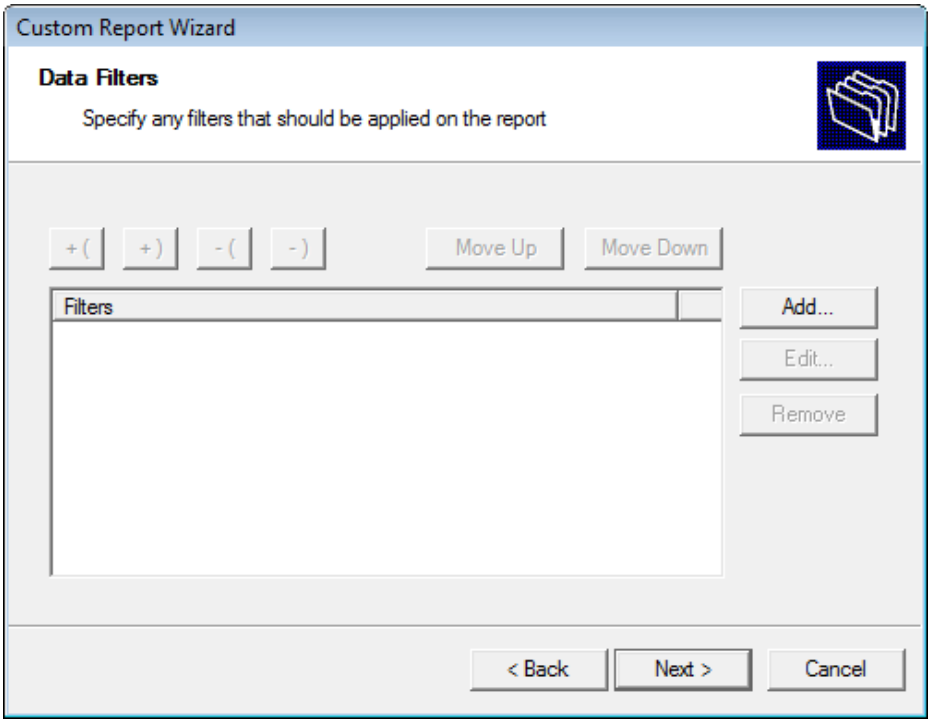
NOTE: For more information on how to configure filter conditions, refer to the section 'Configuring data filter conditions' in this manual.

7. Specify a name and description for the customized report. Click on **Next** to continue.

8. Click on **Finish** to finalize your configuration settings.

4.3 Configuring data filter conditions

Use data filter conditions to specify which network security scan data/results will be included in the report. Only scans which match the specified criteria will be processed and presented within the report.

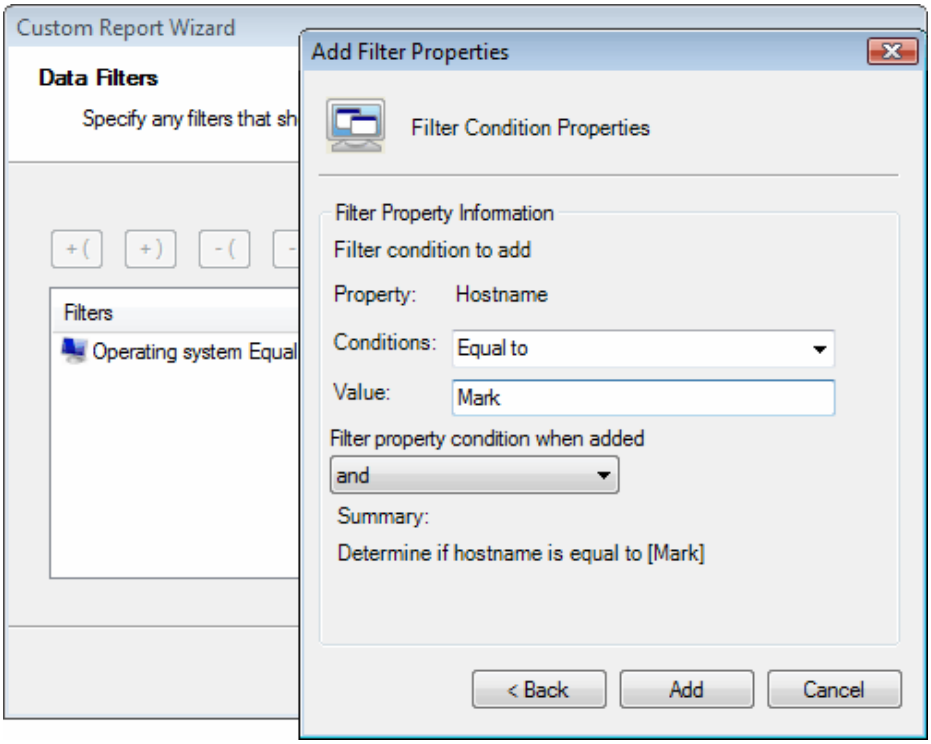


Screenshot 12 - Custom Report Wizard: Filters dialog

Click on the **Add…** button to bring up the 'Edit filter properties' dialog and configure the following conditions:

- **Filter condition** – Specify the data source area on which the filter will focus (for example, select 'Operating System' to filter the events data related to a specific operating system).
- **Condition** – Specify the condition comparison parameter.
- **Value** – Specify the string to which source data will be compared.

For example to generate a report which contains only information related to Windows XP, configure your filter parameters as shown below:



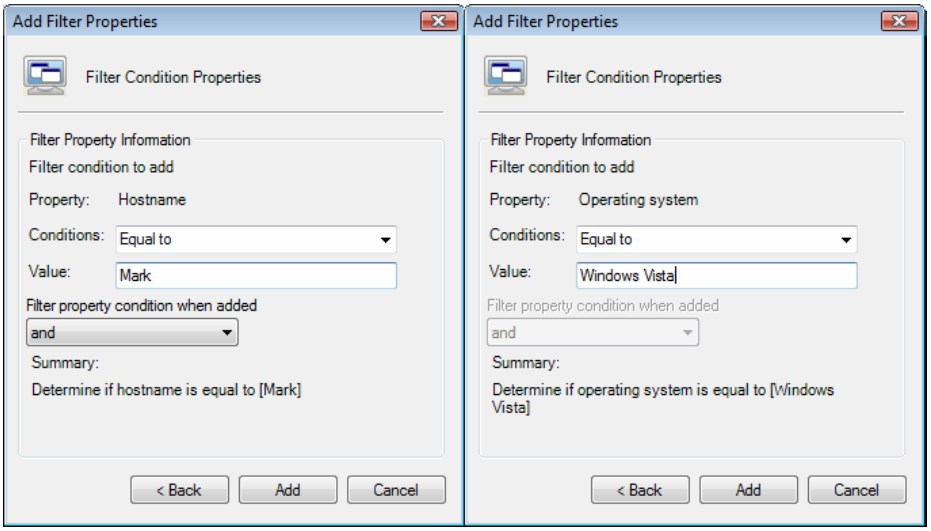
Screenshot 13 - Filter conditions configuration dialog

For more specific reports, you can limit the range of information to be displayed by tightening your conditions/search criteria. This is achieved by configuring and applying multiple data filters against the selected data source. When more than one filter is used, specify how these filters will be logically linked. This is achieved by selecting a logical grouping condition from 'Filter property condition…' drop down list.

- Select **And** to include ALL the scan data information that satisfies ALL of the conditions specified in the filters.
- Select **Or** to include ALL the scan data information that matches at least one of the specified filter conditions.

Example: Using multiple filters

Consider the situation where a custom report has 2 filters configured as follows:



Screenshot 14 - Using multiple filters

Parameters	Filter 1	Filter 2
Filter condition	Hostname	Operating System
Logical relation	Is equal to	Is equal to
Value	'Mark'	'Windows XP'

The data which will be included in this custom report will vary according to how these filters will be applied against your data. This is defined through the 'Filter property condition…' drop-down.

Filters applied			Data output
Filter 1	and	Filter 2	**The report will show:** All scan data which is related to a host called 'Mark' which runs on 'Windows XP'.
Filter 1	or	Filter 2	**The report will show:** All scan data related to 'Windows XP' – (no matter which host it belongs to) AND All scan data related to a host called 'Mark' – (no matter which operating system it has installed).

Example: Creating a custom report based on network security scans performed during a particular month

This example demonstrates how to generate a network vulnerabilities summary report called 'Network vulnerabilities summary on hostname Mark for January 2009'. This report will be based on scans:

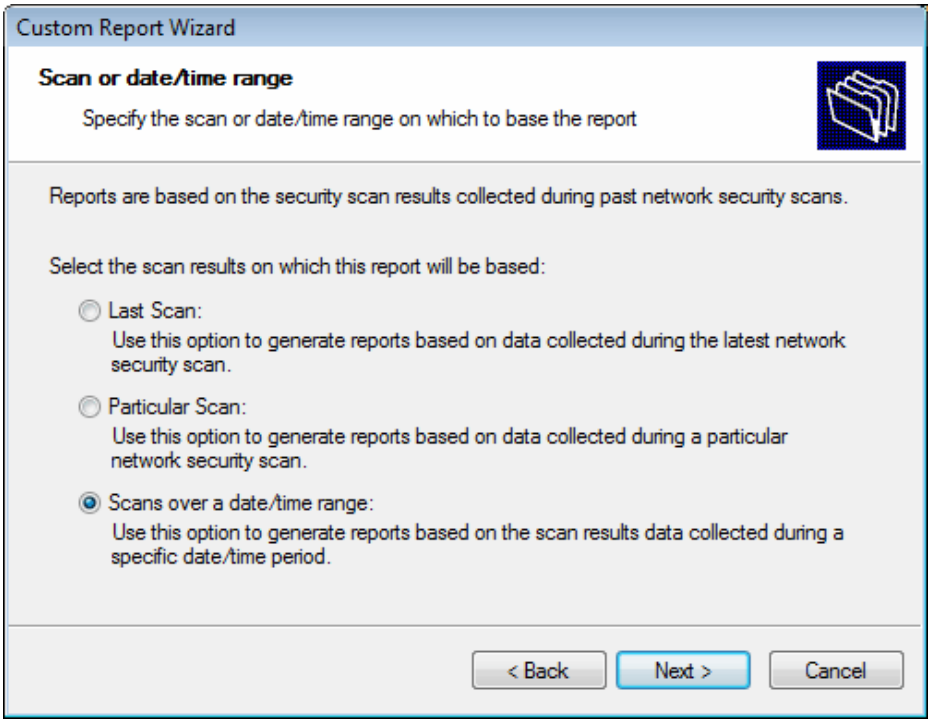
- Related to a host named 'Mark'
- Corresponding to operating system 'Windows XP'
- Performed during the month of 'January 2009'.

To create this report:

1. Click on the **Default Reports** navigation button.

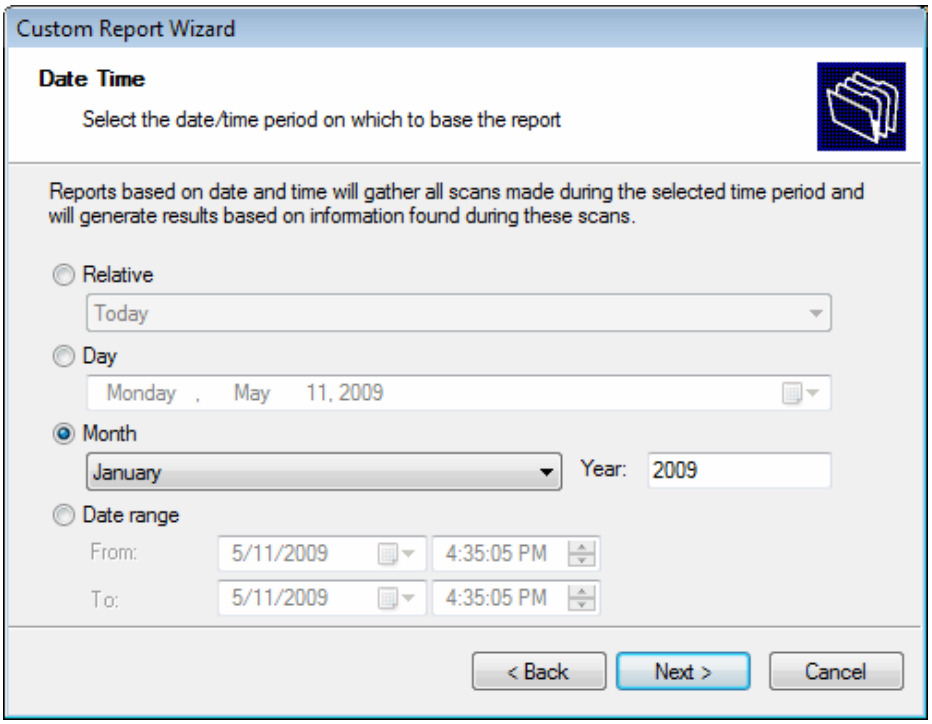
2. Right-click on the report to be customized and select **New ► Custom Report**. This will bring up the 'Custom Reports Wizard'.

3. As soon as the welcome dialog is displayed, click **Next**.


Custom Report Wizard
Scan or date/time range
Specify the scan or date/time range on which to base the report
Reports are based on the security scan results collected during past network security scans.
Select the scan results on which this report will be based:
Last Scan:
Use this option to generate reports based on data collected during the latest network security scan.
Particular Scan:
Use this option to generate reports based on data collected during a particular network security scan.
Scans over a date/time range:
Use this option to generate reports based on the scan results data collected during a specific date/time period.
< Back
Next >
Cancel

Screenshot 15 – Selecting the data source to use

4. Select the **Scans over a date/month range** option and click **Next**.

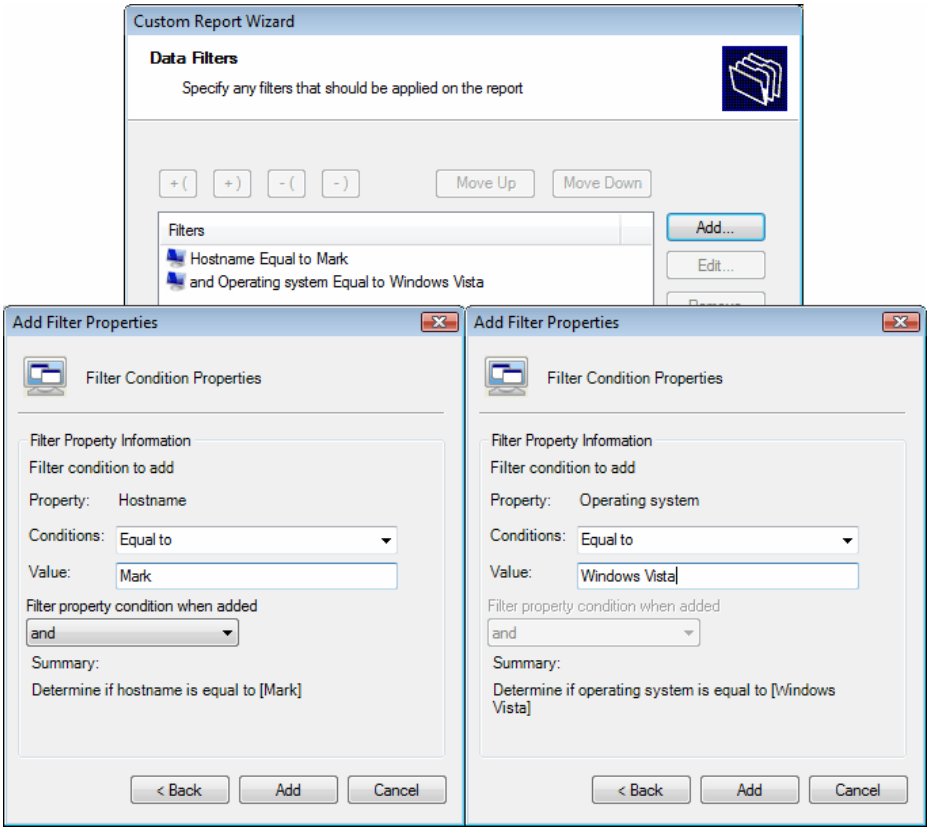

Custom Report Wizard
Date Time
Select the date/time period on which to base the report
Reports based on date and time will gather all scans made during the selected time period and will generate results based on information found during these scans.
Relative
Today
Day
Monday , May 11, 2009
Month
January
Year: 2009
Date range
From: 5/11/2009 4:35:05 PM
To: 5/11/2009 4:35:05 PM
< Back
Next >
Cancel

Screenshot 16 – Selecting the date/time period

5. Select the **Month** option and specify the following parameters:

- **Month**: ‘January’.
- **Year**: ‘2009’.

6. Click on **Next** to proceed to the data filters dialog.



Screenshot 17 - Filter conditions dialog(s)

7. Click on the **Add…** button and configure the parameters of filter 1 as follows:

Filter condition: ‘Hostname’

Condition: ‘Equal to’

Value: ‘Mark’.

8. Click **Add** to finalize your filter configuration settings.

9. Click again on the **Add…** button and configure the parameters of filter 2 as follows:

- **Filter condition:** ‘Operating system’
- **Condition:** ‘is equal to’
- **Value:** ‘Windows Vista’

Filter Property condition…: ‘and’.

10. Click **Add** to finalize your filter configuration settings.

11. Click **Next** and specify the following parameters:

- **Report Name**: ‘Network Vulnerability summary for November 2008’
- **Report Title:** ‘Network security scans of hostname Mark’
- **Report Description**: ‘This report shows a summary of vulnerabilities found on hostname Mark during November 2008.’

12. Click **Next** to proceed to the final dialog.

13. Click **Finish** to finalize your custom report configuration settings.

4.4 Run a custom report

To run a custom report:

1. Click on the **Custom Reports** navigation button.

2. Right-click on the custom report to be generated and select **Generate**.

4.5 Editing a custom report

To edit the configuration settings of a custom report:

1. Click on the **Custom Reports** navigation button.

Custom Report Wizard
Welcome to the LANguard Custom Report Wizard
This wizard will help generate a new customized report based on the following report:
Network Vulnerability Summary (1)
This report is an executive summary showing vulnerability counts for different categories. The report also identifies the top most vulnerable host machines and products, as well as the most common vulnerabilities detected on the network ...
You will be asked to select which security scan data source to use and which filters to apply to this new custom report.
Click next to continue.
< Back
Next >
Cancel

Screenshot 18 - Custom Report Wizard: Welcome dialog

2. Right-click on the custom report to be modified and select **Edit**. This will bring up the 'Custom Reports Wizard' through which you can make the required changes.

NOTE: For more information on how to configure the parameters of a custom report refer to the 'Creating a custom report' section in this chapter.

4.6 Deleting a custom report

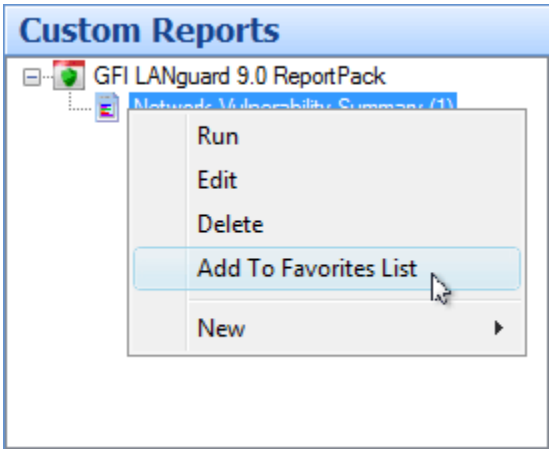
To delete a custom report:

1. Click on the **Custom Reports** navigation button.

2. Right-click on the custom report to be permanently removed from the list and select **Delete**.

3. Click **Yes** to confirm.

4.7 Adding custom reports to the list of favorite reports



Screenshot 19 - Favorite reports navigation button

You can group and access frequently used reports through the **Favorite Reports** navigation button. To add a custom report to the list of favorite reports:

1. Click on the **Custom Reports** navigation button to bring up the list of available reports.

2. Right-click on the custom report to be added to favorites and select **Add to Favorites List**.

3. Click **Yes** to confirm.

5. Scheduling reports

5.1 Introduction

GFI ReportCenter allows you to generate reports on a pre-defined schedule as well as at specified intervals. This way you can automate the generation of reports that are required on regular basis/ periodically.

Further to this, GFI ReportCenter can also be configured to automatically distribute scheduled reports via email. For every scheduled report, you can configure custom emailing parameters including the list of report recipients and the file format (e.g. PDF) in which the report will be attached to the email.

Use the report scheduling feature to automate your report generation requirements. For example, you can schedule lengthy reports after office working hours and automatically email them to the intended recipients. This way, you maximize the availability of your system resources during working hours and avoid any possible disruptions to workflow.

Both default and custom reports can be scheduled for automatic generation.

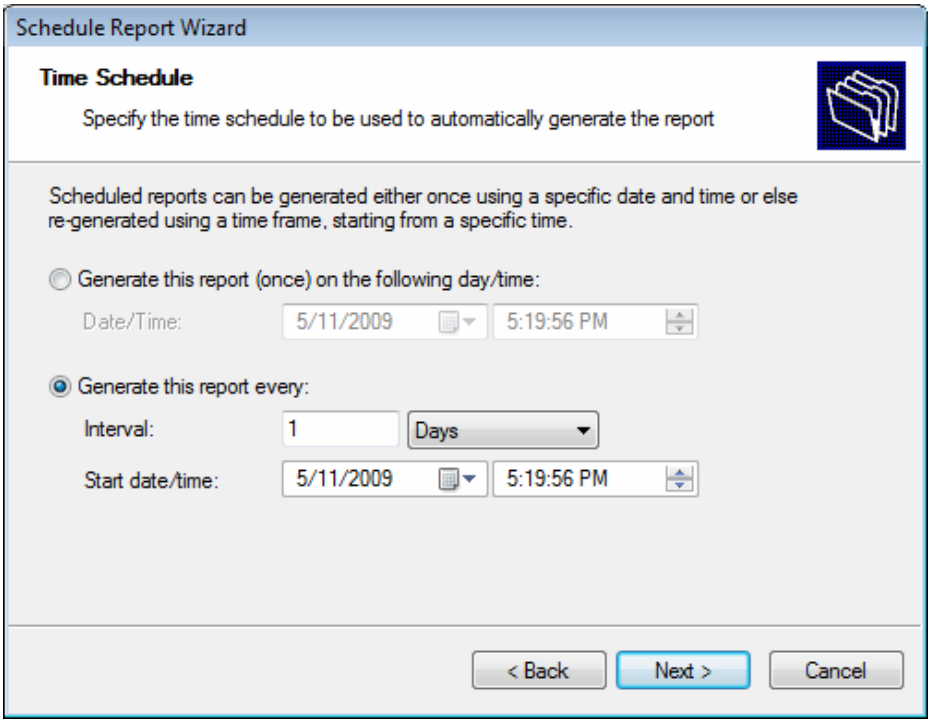
5.2 Scheduling a report

To schedule a report:

1. Click on the **Default/Custom Reports** option pane.

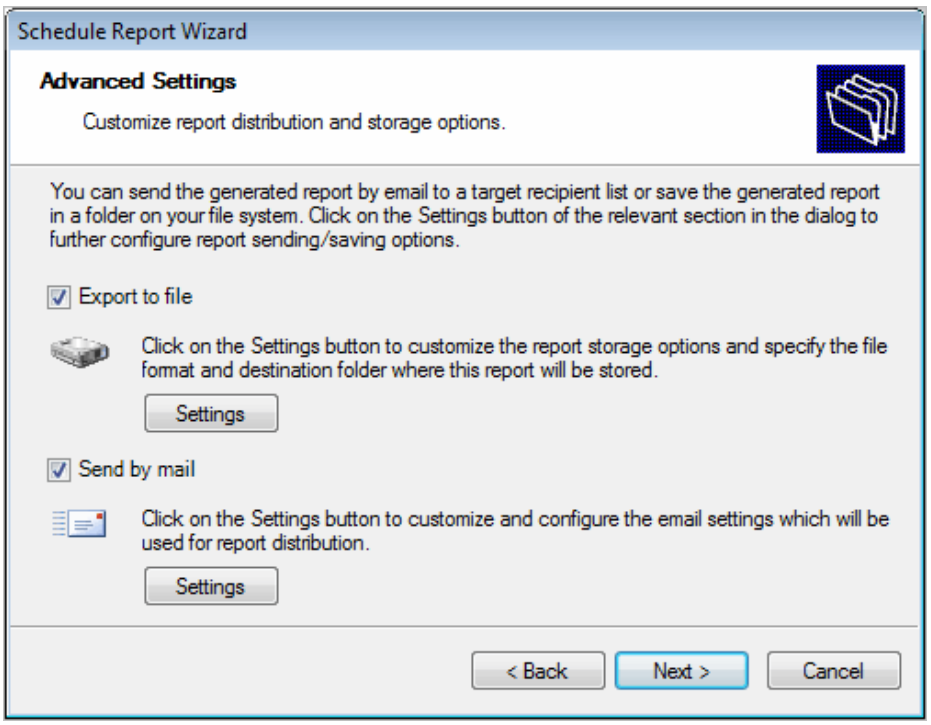
2. Right-click on the report to be scheduled and select **New ► Scheduled report**. This will bring up the 'Scheduled Report Wizard'. Click on **Next** to continue.

3. Select the network security scan(s) data to be covered by this report.


Schedule Report Wizard
Time Schedule
Specify the time schedule to be used to automatically generate the report
Scheduled reports can be generated either once using a specific date and time or else re-generated using a time frame, starting from a specific time.
Generate this report (once) on the following day/time:
Date/Time:
5/11/2009
5:19:56 PM
Generate this report every:
Interval:
1
Days
Start date/time:
5/11/2009
5:19:56 PM
< Back
Next >
Cancel

Screenshot 20 – Report Scheduling Wizard: Time schedule dialogue

4. Specify the report scheduling parameters (date/time/frequency). Click on **Next** to continue.


Schedule Report Wizard
Advanced Settings
Customize report distribution and storage options.
You can send the generated report by email to a target recipient list or save the generated report in a folder on your file system. Click on the Settings button of the relevant section in the dialog to further configure report sending/saving options.
Export to file
Click on the Settings button to customize the report storage options and specify the file format and destination folder where this report will be stored.
Settings
Send by mail
Click on the Settings button to customize and configure the email settings which will be used for report distribution.
Settings
< Back
Next >
Cancel

Screenshot 21 – Report Scheduling Wizard: Advanced Settings dialog

5. To export the generated report to file, select the **Export to file** option. To customize the report export configuration settings click on the **Settings** button underneath this option.

NOTE: For information on how to configure export-to-file settings refer to the 'Configuring report export to file options' section in this chapter.

6. To automatically distribute generated reports via email, select the **Send by** mail option. To customize the email settings used for report distribution click on the **Settings** button underneath this option.

NOTE: For information on how to configure email settings refer to the **Configuring report emailing options** in this chapter.

7. Specify a name and description for this scheduled report. Click **Next** to continue.

8. Click **Finish** to finalize your settings.

5.3 Configuring advanced settings

GFI LANguard ReportPack allows you to export scheduled reports to a specific file format as well as to automatically distribute these reports via email. This is achieved using either a set of parameters (e.g. recipient's email addresses) which are specified on the fly during scheduled report configuration or using the default set of report export and distribution parameters configured during the ReportPack installation.

NOTE: The Report Scheduling Wizard is by default configured to use the default set of report export and distribution parameters.

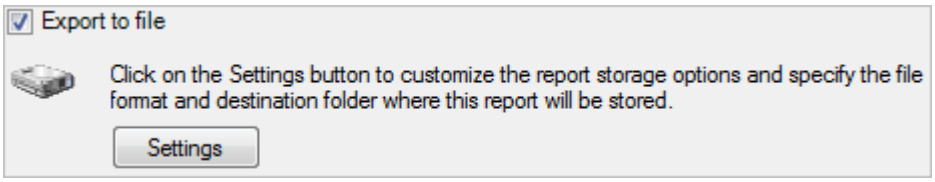
Report export formats

Scheduled reports can be exported in a variety of formats. Supported file formats include:

	Format	Description
1	Adobe Acrobat (.PDF)	Use this format to allow distribution of a report on different systems such as Macintosh and Linux while preserving the layout.
2	MS Excel (.XLS)	Use this format if you want to further process the report and perform more advance calculations using another (external) program such as Microsoft Excel.
3	MS Word (.DOC)	Use this format if you want to access this report using Microsoft Word.
4	Rich text format (.RTF)	Use this format to save the report in a format that is small in size and which allows accessibility through different word processors in different operating systems.

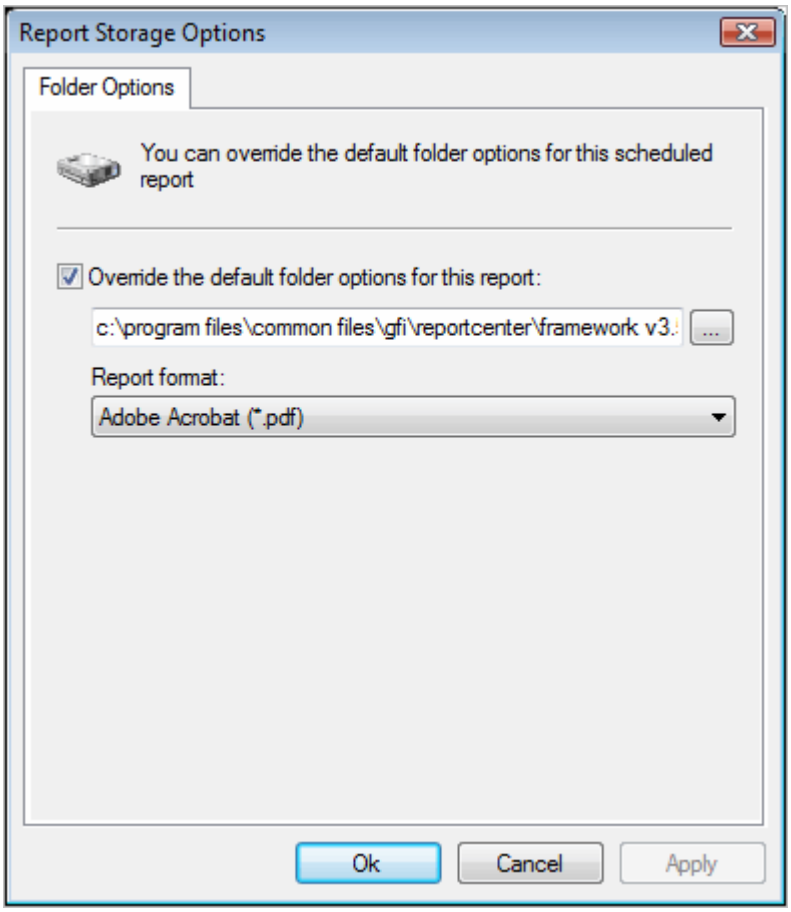
5.3.1 Configuring report export to file options

To configure the report export to file settings of a scheduled report do as follows:


Export to file
Click on the Settings button to customize the report storage options and specify the file format and destination folder where this report will be stored.
Settings

Screenshot 22 - Advanced Settings dialog: Export to file settings button

1. From the **Advanced Settings** dialog, click on the **Settings** button underneath the **Export to file** option.



Screenshot 23 - Advanced Settings: Export to file options

2. Select the option **Override the default folder options for this report:**

3. Specify the complete path where the exported report will be saved.

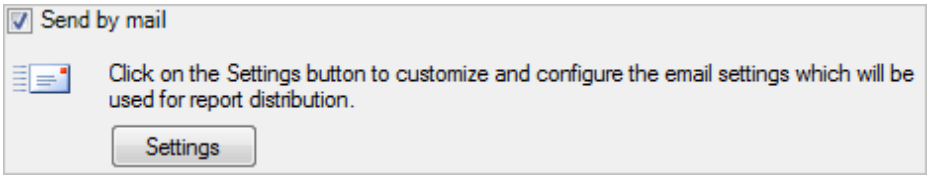
4. Specify the file format in which the exported report will be saved.

5. Click **OK** to finalize your configuration settings.

NOTE: For information on how to configure the default export to file settings refers to the 'Configuring default scheduling options' section in this manual.

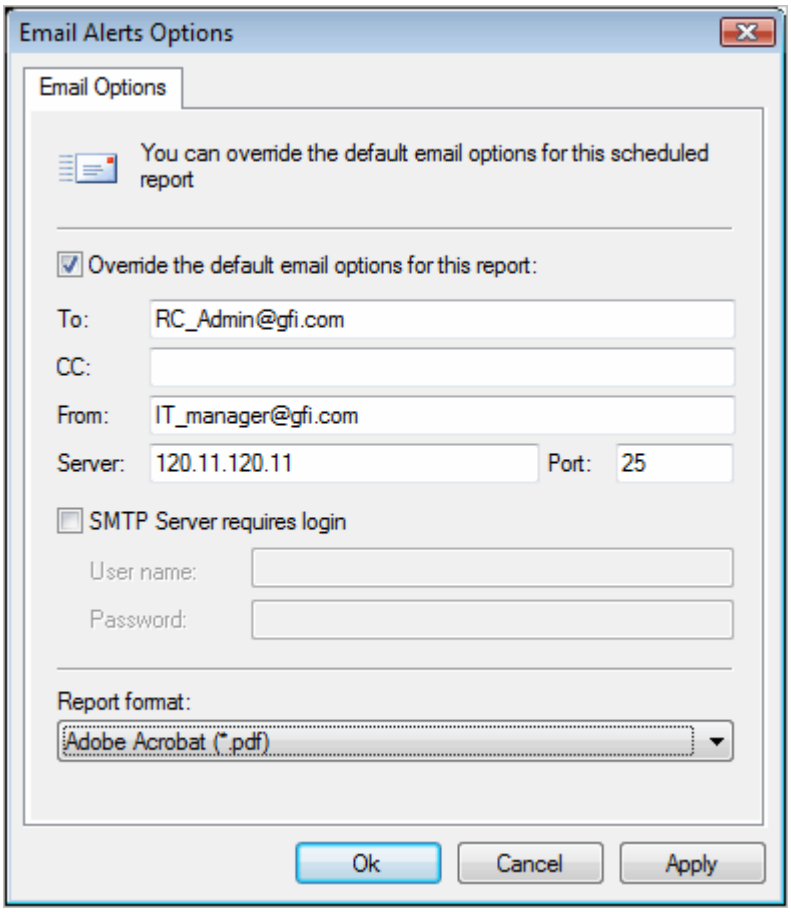
5.3.2 Configuring report emailing options

To configure the report emailing options of a scheduled report do as follows:


Send by mail
Click on the Settings button to customize and configure the email settings which will be used for report distribution.
Settings

Screenshot 24 - Advanced Settings dialog: Send by email settings button

1. From the **Advanced Settings** dialog, click on the **Settings** button underneath the **Send by email** option.



Screenshot 25 - Report distribution options

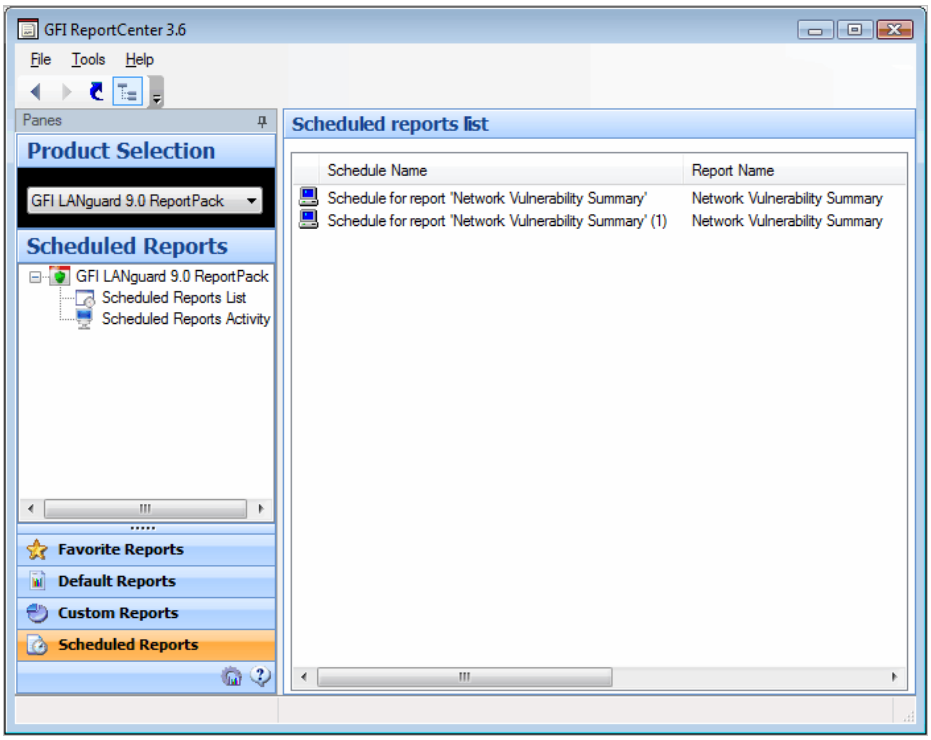
2. Select the option **Override the default email options for this report:**

3. Specify the following parameters:

- **To/CC**: Specify the email address (es) where the generated report will be sent.
- **From**: Specify the email account that will be used to send the report.
- **Server**: Specify the name/IP of your SMTP (outbound) email server. If the specified server requires authentication, select the option **SMTP Server requires login** and specify the logon credentials in the **User name** and **Password** fields.
- **Report format**: Reports are sent via email as attachments. Select the file format in which to send out your report.

4. Click **OK** to finalize your configuration settings.

5.4 Viewing the list of scheduled reports

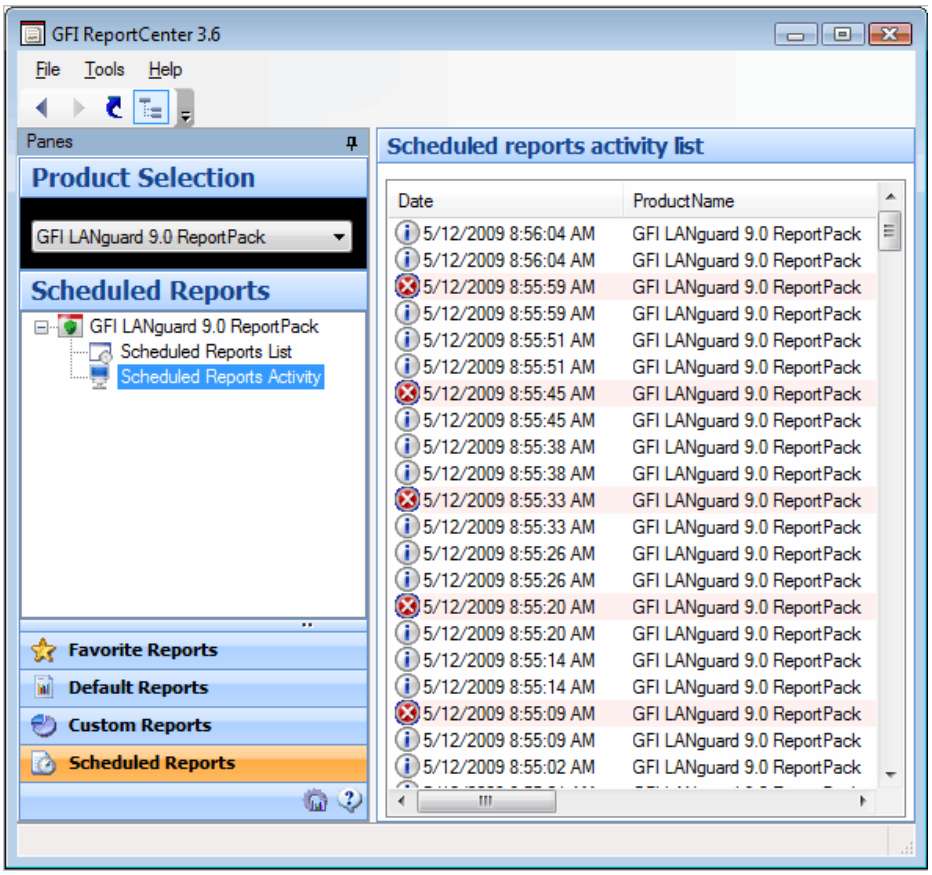


Screenshot 26 - List of Scheduled reports

Click on the **Scheduled Reports** navigation button to show the list of scheduled reports which are currently configured for automatic generation. This information is displayed in the right pane of the management console and includes the following details:

- **Schedule Name:** The custom name that was specified during the creation of the new scheduled report.
- **Report Name:** The names of the default or custom report(s) that will be generate.
- **Last Generation:** Indicates the date/time when the report was last generated.
- **Next Generation:** Indicate the date/time when the report is to be next generated.
- **Description:** The description that you have entered for each schedule.
- **Report Pack:** The GFI LANguard version that created the report.

5.5 Viewing the scheduled reports activity


GFI ReportCenter 3.6
File
Tools
Help
Panes
Product Selection
GFI LANguard 9.0 ReportPack
Scheduled Reports
GFI LANguard 9.0 ReportPack
Scheduled Reports List
Scheduled Reports Activity
Favorite Reports
Default Reports
Custom Reports
Scheduled Reports
Scheduled reports activity list
Date
ProductName
5/12/2009 8:56:04 AM GFI LANguard 9.0 ReportPack
5/12/2009 8:56:04 AM GFI LANguard 9.0 ReportPack
5/12/2009 8:55:59 AM GFI LANguard 9.0 ReportPack
5/12/2009 8:55:59 AM GFI LANguard 9.0 ReportPack
5/12/2009 8:55:51 AM GFI LANguard 9.0 ReportPack
5/12/2009 8:55:51 AM GFI LANguard 9.0 ReportPack
5/12/2009 8:55:45 AM GFI LANguard 9.0 ReportPack
5/12/2009 8:55:45 AM GFI LANguard 9.0 ReportPack
5/12/2009 8:55:38 AM GFI LANguard 9.0 ReportPack
5/12/2009 8:55:38 AM GFI LANguard 9.0 ReportPack
5/12/2009 8:55:33 AM GFI LANguard 9.0 ReportPack
5/12/2009 8:55:33 AM GFI LANguard 9.0 ReportPack
5/12/2009 8:55:26 AM GFI LANguard 9.0 ReportPack
5/12/2009 8:55:26 AM GFI LANguard 9.0 ReportPack
5/12/2009 8:55:20 AM GFI LANguard 9.0 ReportPack
5/12/2009 8:55:20 AM GFI LANguard 9.0 ReportPack
5/12/2009 8:55:14 AM GFI LANguard 9.0 ReportPack
5/12/2009 8:55:14 AM GFI LANguard 9.0 ReportPack
5/12/2009 8:55:09 AM GFI LANguard 9.0 ReportPack
5/12/2009 8:55:09 AM GFI LANguard 9.0 ReportPack
5/12/2009 8:55:02 AM GFI LANguard 9.0 ReportPack

Screenshot 27 - Schedule activity monitor

GFI ReportCenter also includes a schedule activity monitor through which you can view events related to all scheduled reports that have been executed.

To open the schedule activity monitor, click on the **Scheduled Reports** navigation button and select the **Scheduled Reports Activity** node. This will bring up the activity information in the right pane of the GFI ReportCenter management console.

The activity monitor displays the following events:

	Information: The scheduled report was successfully executed and sent by email and/or saved to disk.
	Warning: The scheduled report was not executed because product license is invalid or has expired.
	Error: The scheduled report was not executed due to a particular condition/event. Typical conditions include:

- Errors when attempting to save the generated report to a specific folder (for example, out of disk space).
- Errors when attempting to send the generated report via email (for example, the SMTP server configured in the GFI ReportCenter settings is not reachable).

The activity monitor records and enumerates the following information:

- **Date:** The date and time when the scheduled report was executed.
- **Product name**: The name of the GFI product to which the report belongs.
- **Type:** The event classification - error, information, or warning.
- **Description:** Information related to the state of a scheduled report that has been executed. The format and contents of the activity description vary, depending on the event type.

NOTE: The description is often the most useful piece of information, indicating what happened during the execution of a scheduled report or the significance of the event.

5.6 Enable/disable a scheduled report

Scheduled reports can be enabled or disabled as required. Use the **Scheduled Reports** navigation button to view the list of scheduled reports as well as to identify their current status. The status of scheduled reports is shown through the icon included on the left hand side of each schedule:

	Indicates that the scheduled report is disabled.
	Indicates that the scheduled report is enabled/pending.

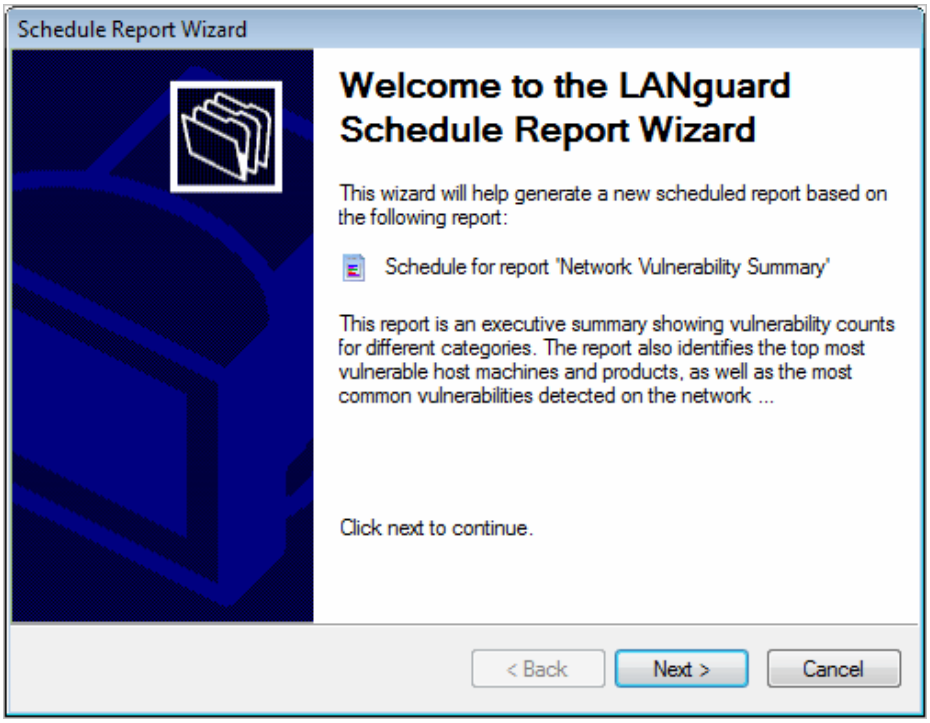
To enable or disable a scheduled report, right-click on the respective report and select **Enable/Disable** accordingly.

5.7 Editing a scheduled report

To make changes to the configuration settings of a scheduled report:

1. Click on the **Scheduled Reports** navigation button.

2. Right-click on the scheduled report to be re-configured and select **Properties**. This will bring up the 'Scheduled Reports Wizard'.


Schedule Report Wizard
Welcome to the LANguard Schedule Report Wizard
This wizard will help generate a new scheduled report based on the following report:
Schedule for report 'Network Vulnerability Summary'
This report is an executive summary showing vulnerability counts for different categories. The report also identifies the top most vulnerable host machines and products, as well as the most common vulnerabilities detected on the network ...
Click next to continue.
< Back
Next >
Cancel

Screenshot 28 - Scheduled Reports wizard

3. Click on **Next** and perform the required changes. For information on how to configure the parameters of a scheduled report refer to the 'Creating a scheduled report' section in this chapter.

Deleting a scheduled report

To delete a scheduled report:

1. Click on the **Scheduled Reports** navigation button.

2. Right-click on the scheduled report to be permanently removed from the list and select **Delete**.

5.8 Example: Scheduling a report

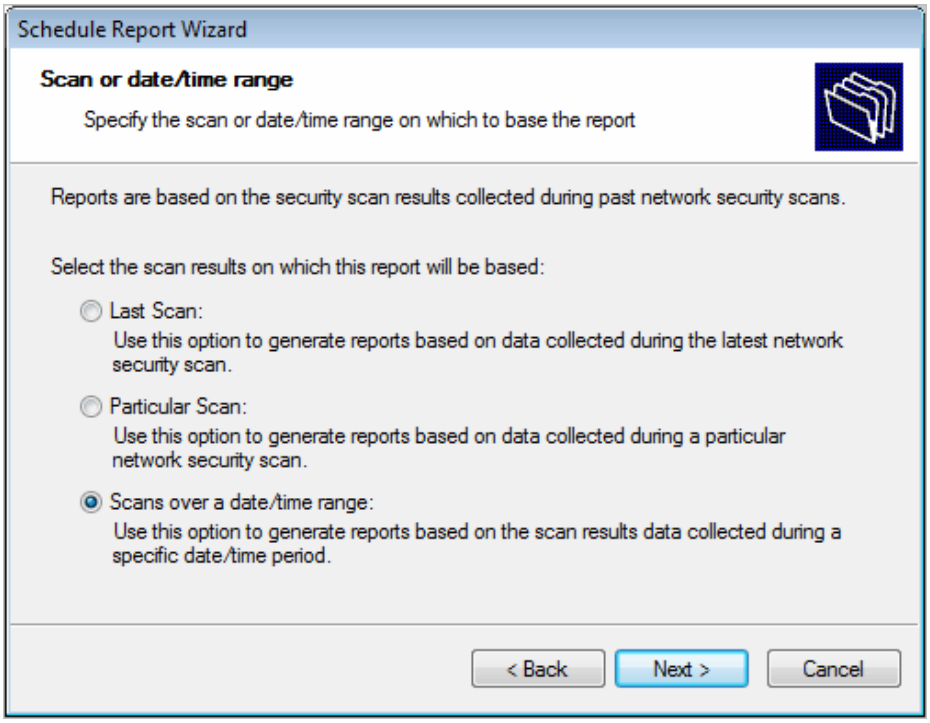
This example demonstrates how to schedule a software audit report which will:

- Generate the first report on 5/12/2009 at 8:00:00 PM.
- Continue generating the same report on a monthly basis.
- Export the generated report(s) to folder 'C:\Monthly Reports' in PDF format.
- Email the generated report using the following custom parameters:
- Send from email account: 'RC_Admin@gfi.com'
- Send to email account: 'IT_manager@gfi.com'
- SMTP server details: '120.11.120.11.

To create the scheduled report:

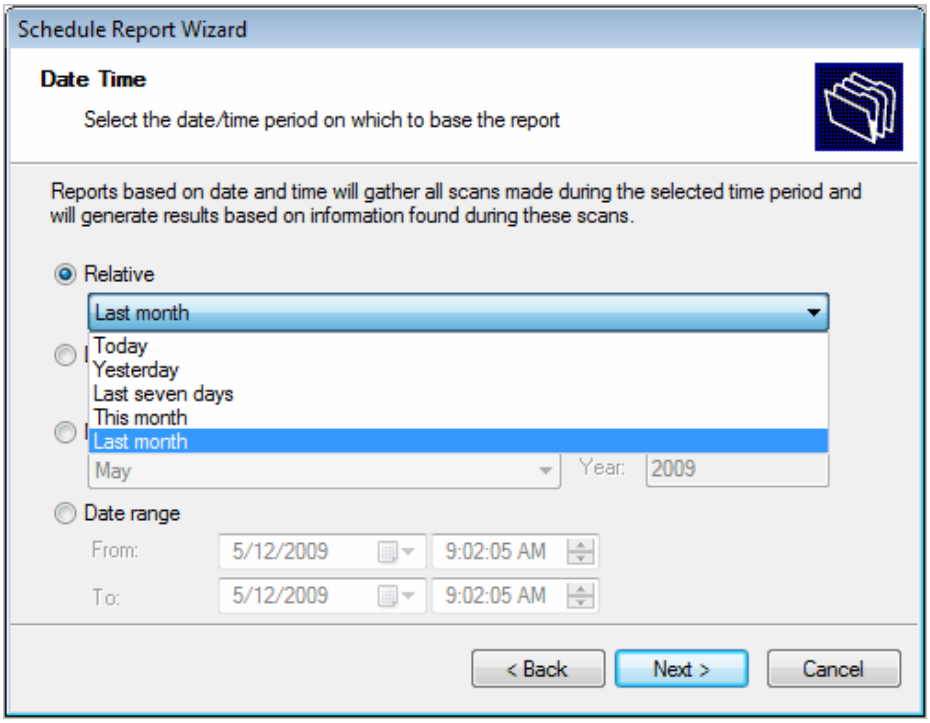
1. Click on the **Default Reports** navigation button.

2. Right-click on **Network Vulnerability Summary** and select **New ► Scheduled Report**. As soon as the welcome dialog is displayed click Next.


Schedule Report Wizard
Scan or date/time range
Specify the scan or date/time range on which to base the report
Reports are based on the security scan results collected during past network security scans.
Select the scan results on which this report will be based:
Last Scan:
Use this option to generate reports based on data collected during the latest network security scan.
Particular Scan:
Use this option to generate reports based on data collected during a particular network security scan.
Scans over a date/time range:
Use this option to generate reports based on the scan results data collected during a specific date/time period.
< Back
Next >
Cancel

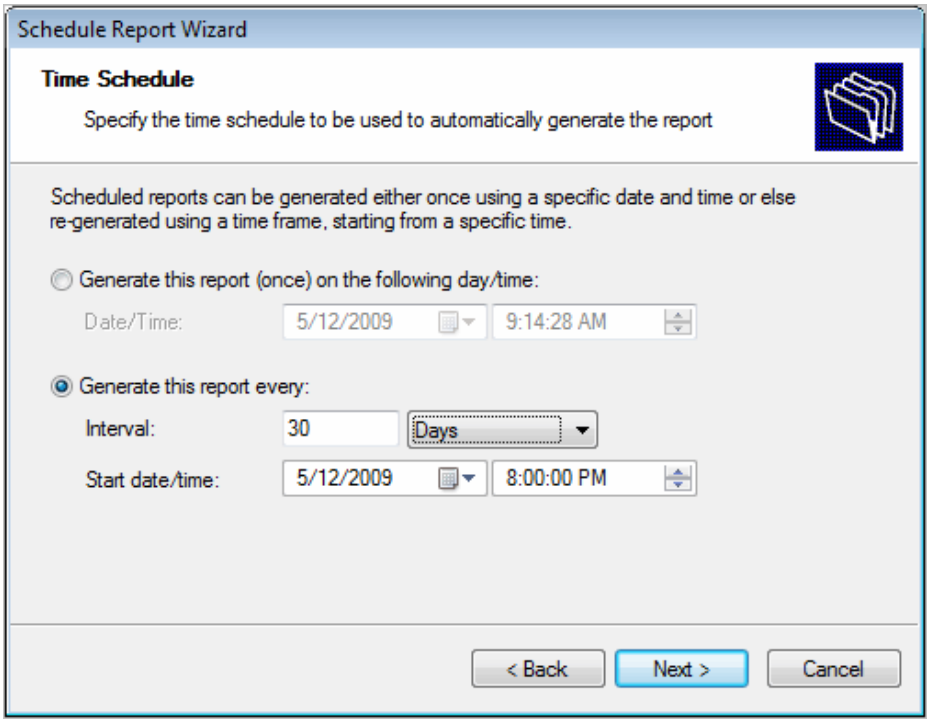
Screenshot 29 - Select network security scan(s) data

3. Select the option **Scans over a date/time range** for data to be covered by this report and click **Next**.



Screenshot 30 - Select date/time of network scan

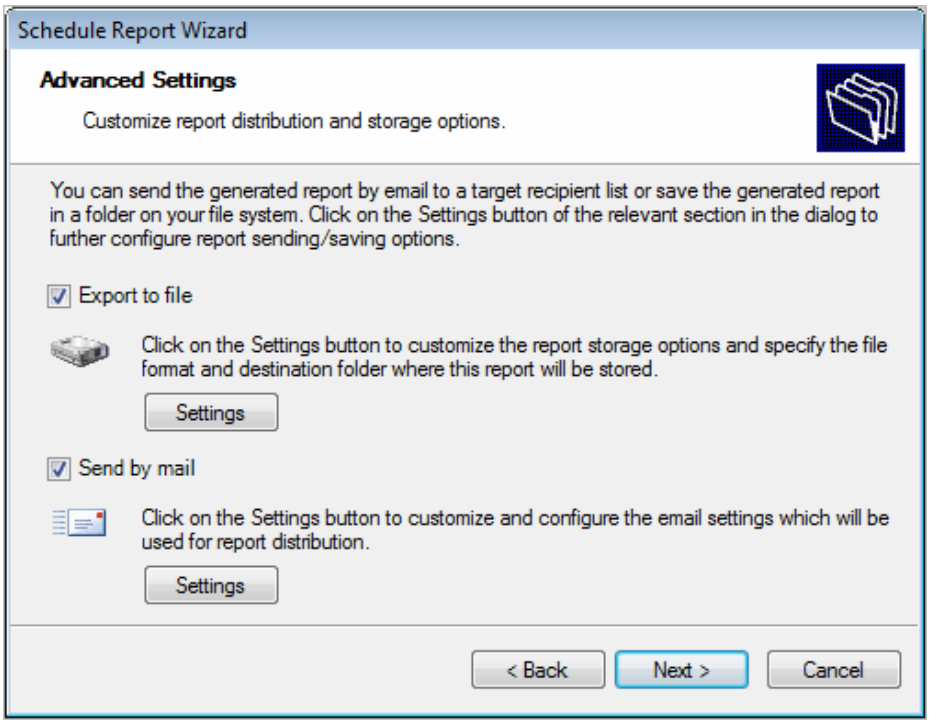
4. Select the option **Relative** and from the provided drop down list select **Last month**. Click on **Next** to proceed to the next dialog.


Schedule Report Wizard
Time Schedule
Specify the time schedule to be used to automatically generate the report
Scheduled reports can be generated either once using a specific date and time or else re-generated using a time frame, starting from a specific time.
Generate this report (once) on the following day/time:
Date/Time:
5/12/2009
9:14:28 AM
Generate this report every:
Interval:
30
Days
Start date/time:
5/12/2009
8:00:00 PM
< Back
Next >
Cancel

Screenshot 31 – Specifying the scheduling options

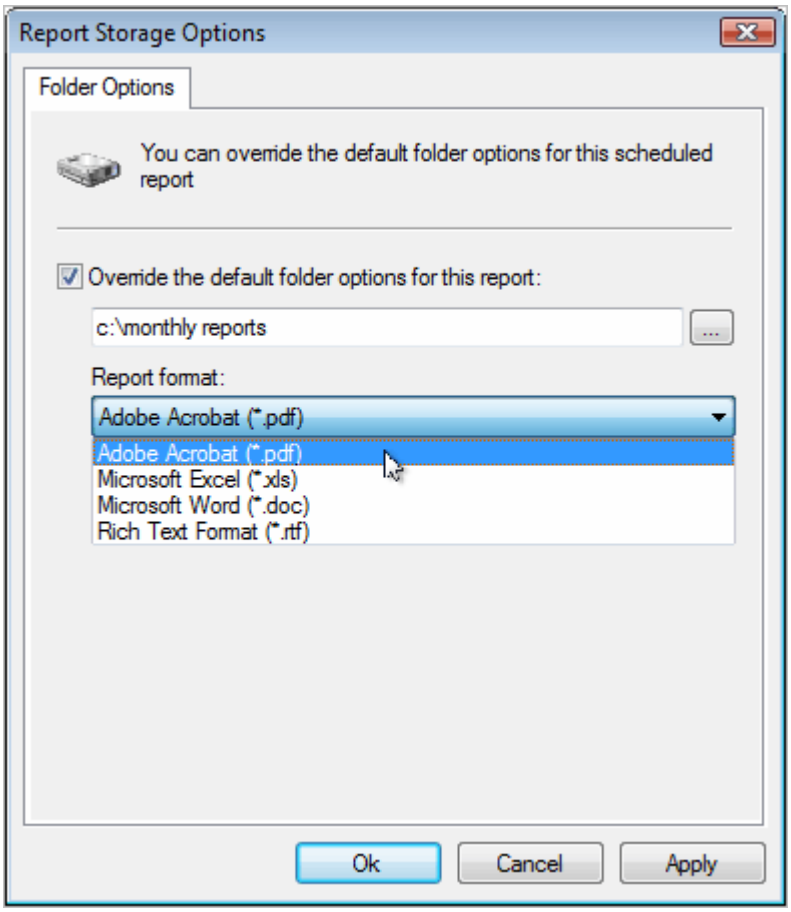
5. To generate this report on a monthly basis, select the option **Generate this report every:** and set the interval to **30 Days**.

6. Set the start date to '5/12/2009' and time to '8:00:00 PM'. Click **Next** to continue.


Schedule Report Wizard
Advanced Settings
Customize report distribution and storage options.
You can send the generated report by email to a target recipient list or save the generated report in a folder on your file system. Click on the Settings button of the relevant section in the dialog to further configure report sending/saving options.
Export to file
Click on the Settings button to customize the report storage options and specify the file format and destination folder where this report will be stored.
Settings
Send by mail
Click on the Settings button to customize and configure the email settings which will be used for report distribution.
Settings
< Back
Next >
Cancel

Screenshot 32 - Advanced Settings dialog

7. From the **Advanced Settings** dialog, click on the **Settings** button underneath the **Export to file** option.

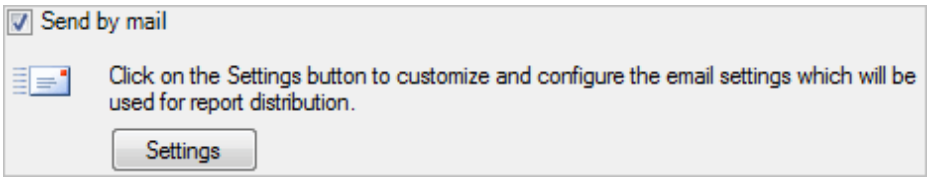


Screenshot 33 - Advanced Settings: Export to file options

8. Select the option **Override the default folder options for this report**:

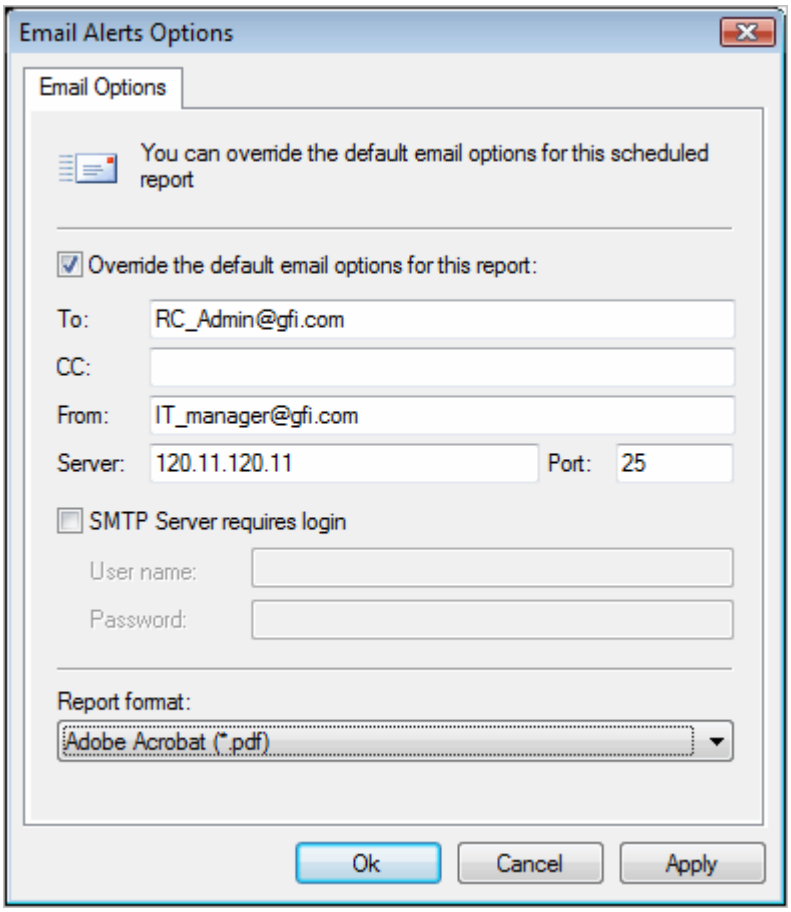
9. Specify the complete path where this report will be saved i.e. 'C:\Monthly Reports'.

10. From the report format drop down select **PDF** and click **OK**.


Send by mail
Click on the Settings button to customize and configure the email settings which will be used for report distribution.
Settings

Screenshot 34 - Advanced Settings dialog: Send by email settings button

11. From the **Advanced Settings** dialog, click on the **Settings** button underneath the **Send by email** option.



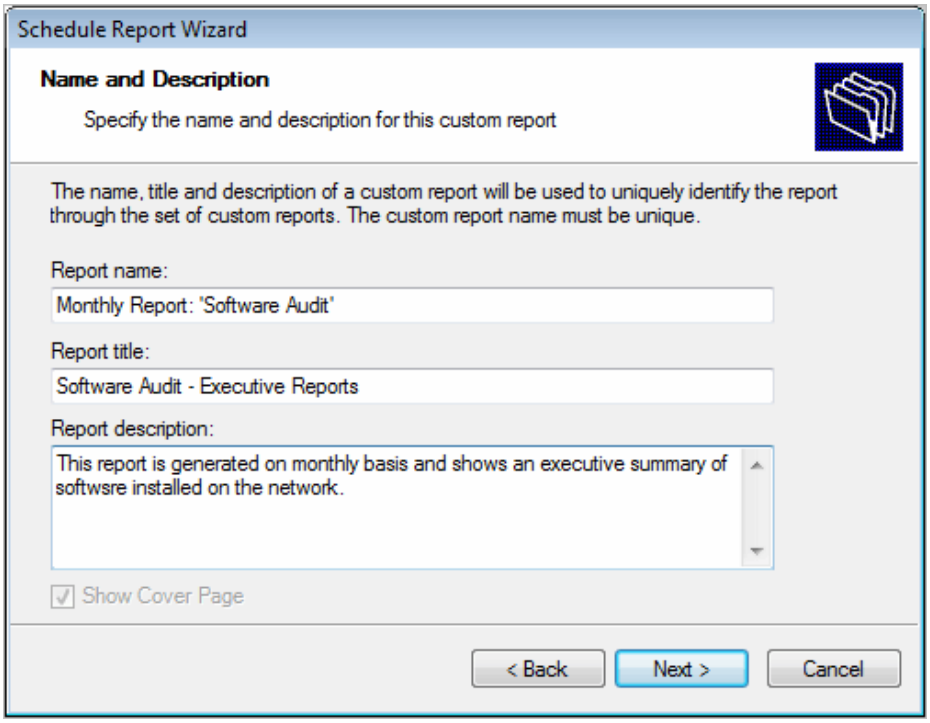
Screenshot 35 - Report distribution options

12. Select the option **Override the default email options for this report:**

13. Specify the following parameters:

- **To:** 'RC_Admin@gfi.com'
- **From:** 'IT_manager@gfi.com'
- **Server:** '120.11.120.11'.

14. From the report format drop down select **PDF** and click **OK** to finalize your email settings.


Schedule Report Wizard
Name and Description
Specify the name and description for this custom report
The name, title and description of a custom report will be used to uniquely identify the report through the set of custom reports. The custom report name must be unique.
Report name:
Monthly Report: 'Software Audit'
Report title:
Software Audit - Executive Reports
Report description:
This report is generated on monthly basis and shows an executive summary of softwsre installed on the network.
Show Cover Page
< Back
Next >
Cancel

Screenshot 36 – Custom report name and description

15. Click **Next** and specify the following parameters:

- **Report Name**: 'Monthly report: 'Software Audit'
- **Report Title**: 'Software Audit – Executive reports'
- **Report Description**: This report is generated on a monthly basis and shows an executive summary of software installed on the network.

16. Click **Next** to proceed to the final dialog.
17. Click **Finish** to finalize your custom report configuration settings.

6. Configuring default options

6.1 Introduction

The GFI LANguard ReportPack allows you to configure a default set of parameters which can be used when generating reports. These parameters are first set during installation. However, you can still reconfigure any of these parameters via the **Options** navigation button and the **Tools** menu provided in the GFI ReportCenter management console.

Screenshot 37 - Options navigation button and Tools menu

Through the **Options** navigation button you can configure the following parameter:

Database source: Use this node to specify the database backend from where the ReportPack will extract the required reporting data.

Through the **Tools** menu you can configure the following parameters:

- **Default scheduling settings:** Use this menu option to configure the default export to file parameters and report emailing parameters of scheduled reports.

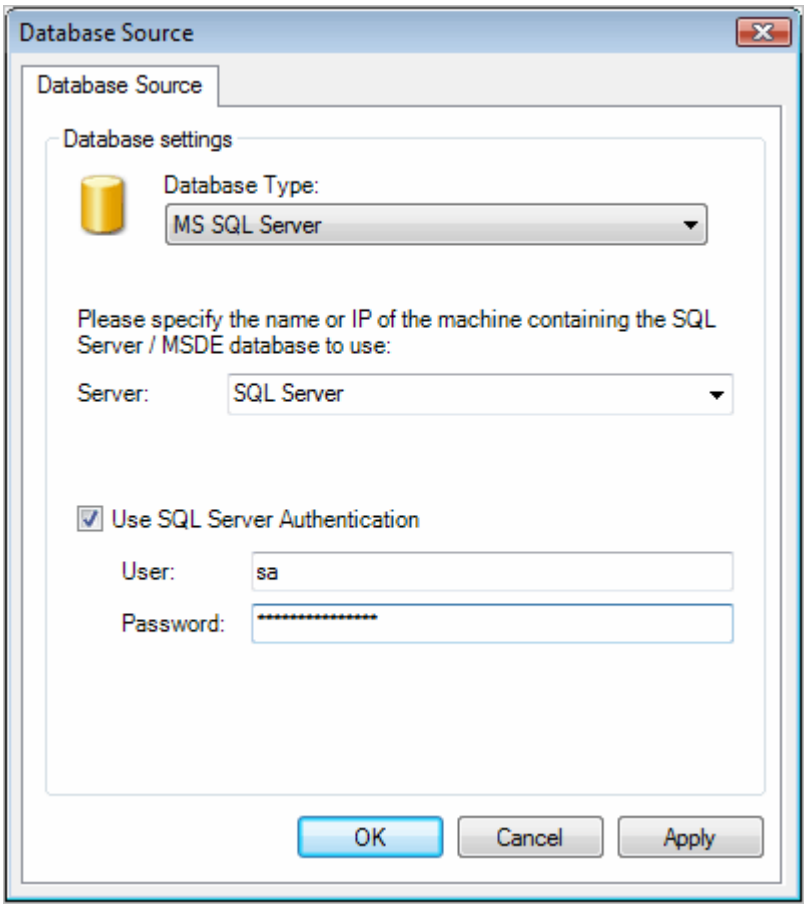
You can also backup your configuration settings for the ReportPack through the **Import/Export Configuration** node in the **Options** section. Exported configurations may be imported into a separate GFI ReportCenter instance, provided that the same ReportPacks are installed on both instances.

6.2 Configuring database source: Microsoft SQL Server

To configure MS SQL Server your database source:

1. Click on the **Options** navigation button.

2. Right-click on the **Database Source** node and select **Set Database Source…** This will bring up the database source configuration dialog.



Screenshot 38 - Database source configuration dialog: SQL Server

3. Select **MS SQL Server** as the database type from the provided list of supported databases.

4. Specify the name or IP address of your MSDE/MS SQL Server database backend.

5. To use the credentials of an SQL Server account, select the **Use SQL Server authentication** option and specify the user name and password in the provided fields.

NOTE: By default, the GFI LANguard ReportPack uses Windows logon credentials to authenticate to the SQL Server.

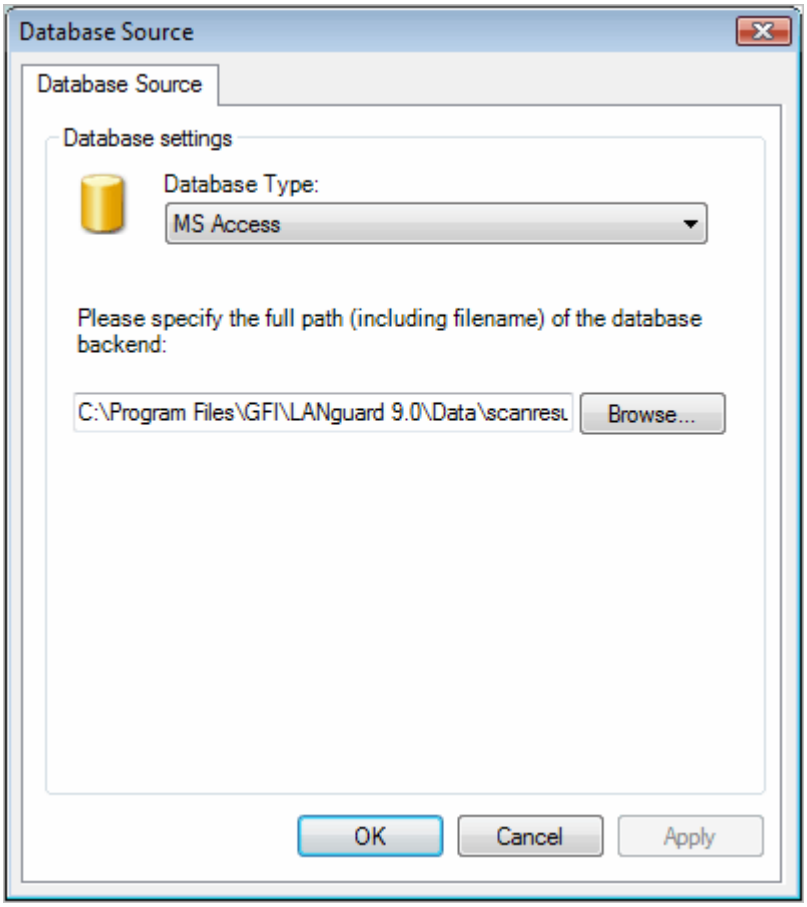
6. Click on **OK** to finalize your configuration settings.

6.3 Configuring database source: Microsoft Access

To configure Microsoft Access as your database source:

1. Click on the **Options** navigation button.

2. Right-click on the **Database Source** node and select **Set Database Source…** This will bring up the database source configuration dialog.



Screenshot 39 - Database source configuration dialog: MS Access

3. Select **MS Access** as the database type from the provided list of supported databases.

4. Specify the complete path to the database backend. If the database source is not stored locally, specify the complete path using Universal Naming Convention (UNC).

(e.g.\\Security_Server\Program Files\GFI\LANguard9\ Data\scanresult.mdb).

5. Click on **OK** to finalize your configuration settings.

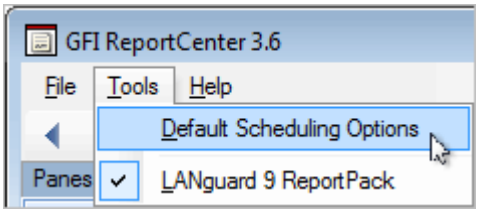
6.4 Viewing the current database source settings

Screenshot 40 - Database source configuration settings

After configuration, you can view the current database source settings by clicking on the **Database Source** node.

6.5 Configuring default scheduling settings

To configure the default settings to be used by scheduled reports:

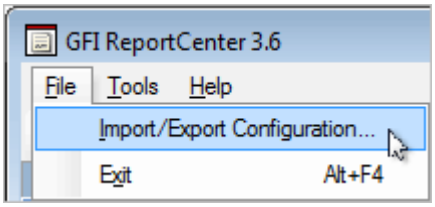


Screenshot 41 - Default scheduling options node

1. From the pull-down menu, click on the **Tools ► Default Scheduling Options**.

2. Configure the required parameter as described in the 'Configuring Advanced Settings' section of the Scheduling Reports chapter.

6.6 Importing/Exporting the configuration



Screenshot 42 – Import/Export Configuration node

The GFI ReportCenter allows you to backup your configuration settings for the ReportCenter and all ReportPacks through **Import/Export Configuration…** in the **File** pull-down menu. Settings are exported for:

- Default scheduling options
- Custom reports
- Scheduled reports
- Favorite reports.

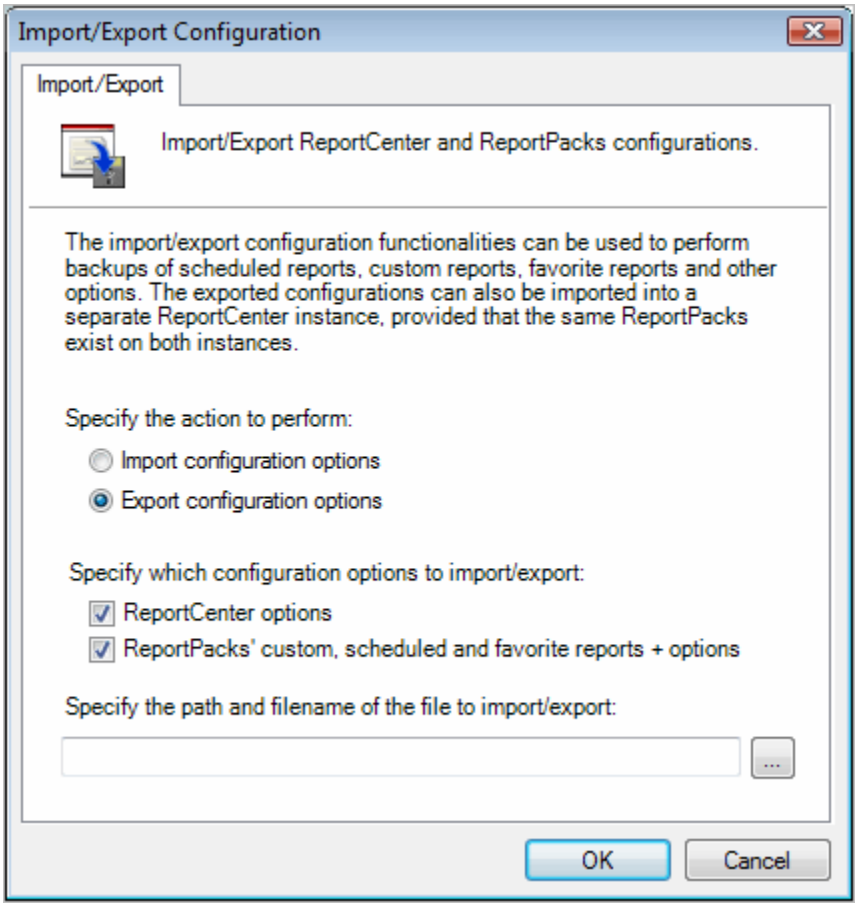
The configuration is backed up into an XML file which may be imported into a separate GFI ReportCenter instance, provided that the same ReportPacks are installed on both instances.

You can also import/export the configuration for a particular ReportPack through the **Import/Export Configuration** node in the **Options** section of the ReportPack

.

Exporting the configuration

To export the GFI LANguard configuration:


Import/Export Configuration
Import/Export
Import/Export ReportCenter and ReportPacks configurations.
The import/export configuration functionalities can be used to perform backups of scheduled reports, custom reports, favorite reports and other options. The exported configurations can also be imported into a separate ReportCenter instance, provided that the same ReportPacks exist on both instances.
Specify the action to perform:
Import configuration options
Export configuration options
Specify which configuration options to import/export:
ReportCenter options
ReportPacks' custom, scheduled and favorite reports + options
Specify the path and filename of the file to import/export:
...
OK
Cancel

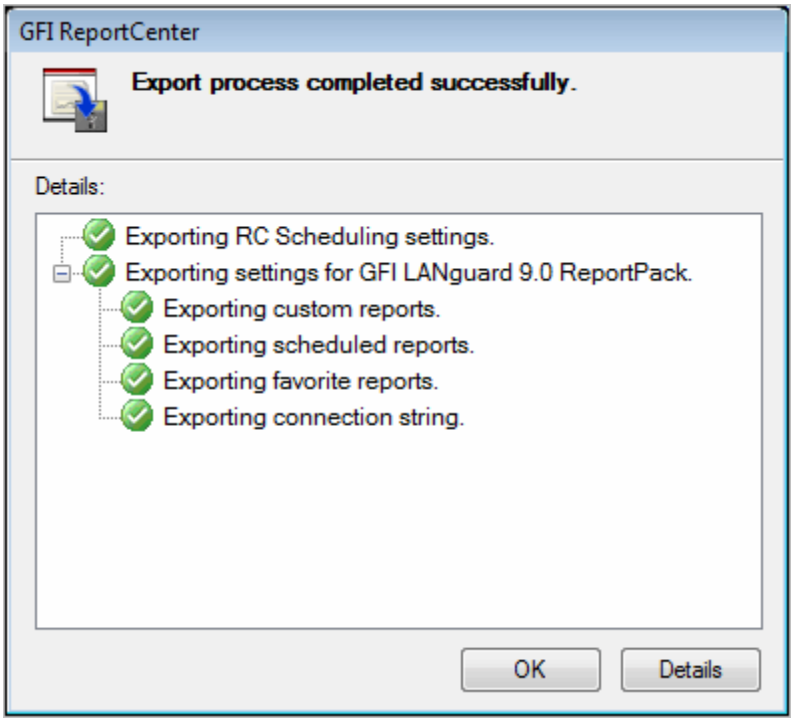
Screenshot 43 – Import/Export configuration dialog

1. From the pull-down menu, click on the **File ► Import/Export Configuration…** . This will bring up the configuration dialog.

2. Select the option **Export configurations options**.

3. Specify which configuration options to export.

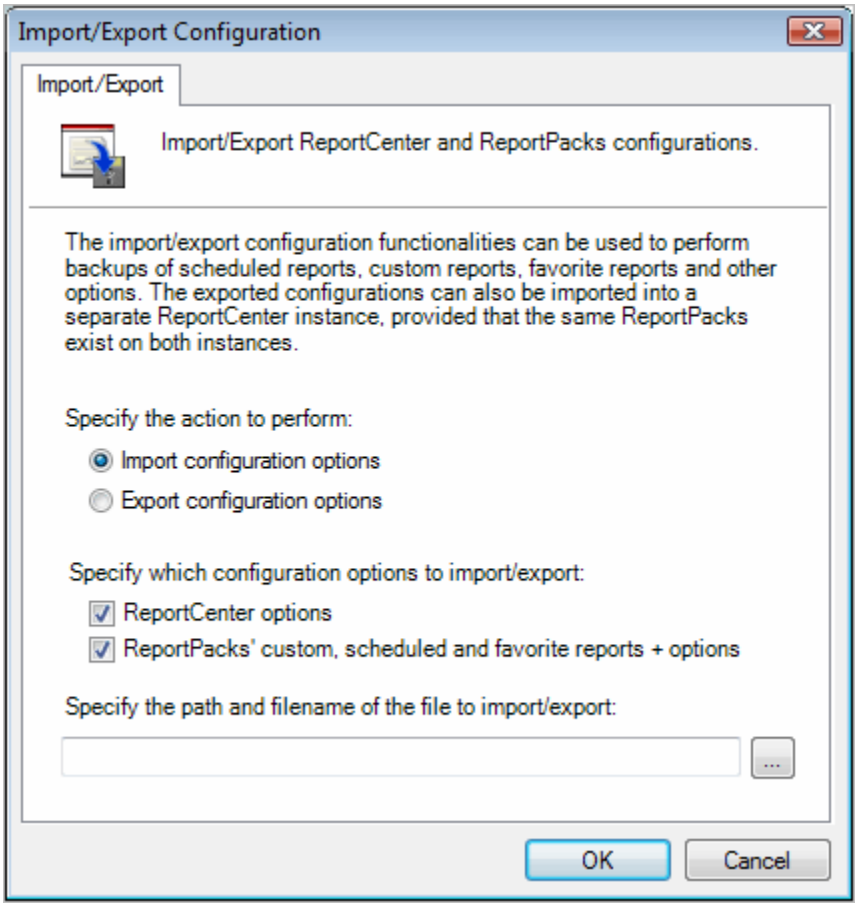
4. Specify the path and filename of the XML file to export. Click on **OK** to proceed with the export.



Screenshot 44 – Export configuration success

Importing the configuration

To import the GFI LANguard configuration:


Import/Export Configuration
Import/Export
Import/Export ReportCenter and ReportPacks configurations.
The import/export configuration functionalities can be used to perform backups of scheduled reports, custom reports, favorite reports and other options. The exported configurations can also be imported into a separate ReportCenter instance, provided that the same ReportPacks exist on both instances.
Specify the action to perform:
Import configuration options
Export configuration options
Specify which configuration options to import/export:
ReportCenter options
ReportPacks' custom, scheduled and favorite reports + options
Specify the path and filename of the file to import/export:
...
OK
Cancel

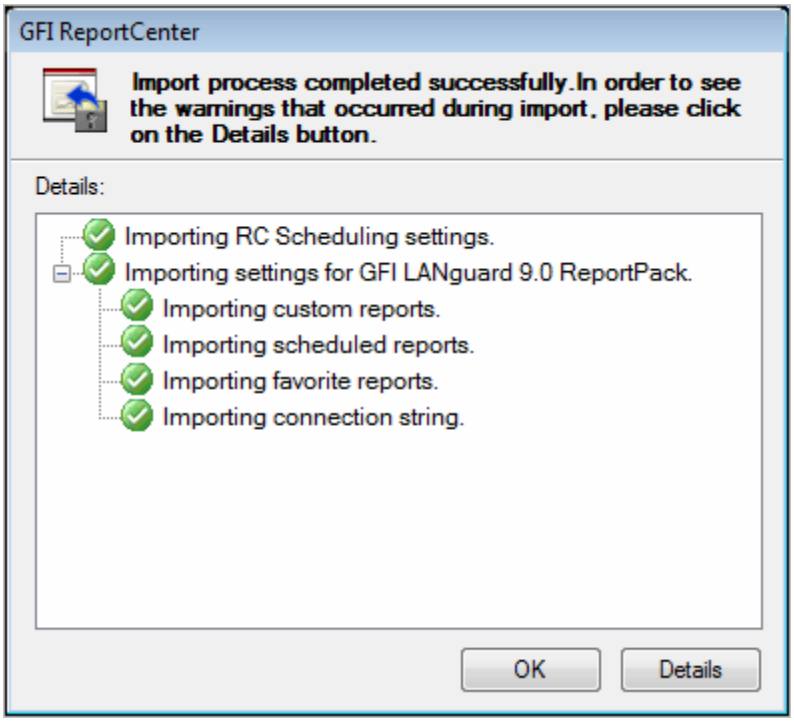
Screenshot 45 – Import configurations dialog

1. From the pull-down menu, click on the **File ► Import/Export Configuration…** . This will bring up the configuration dialog.

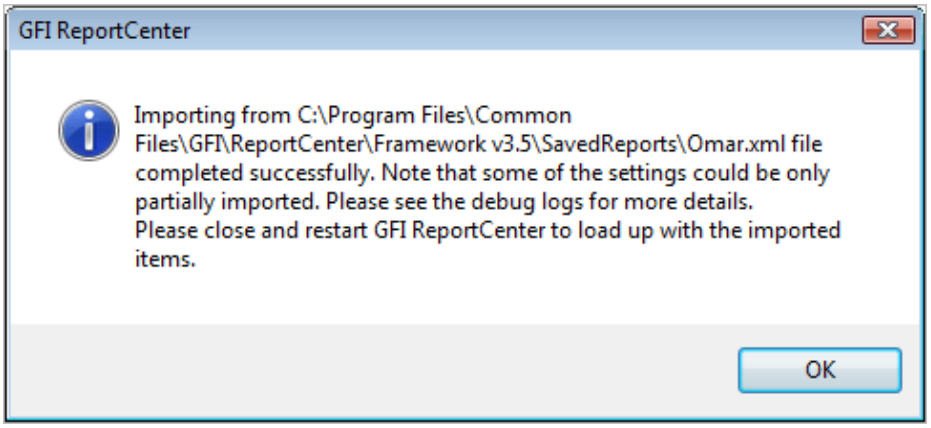
2. Select the option **Import configurations options**.

3. Specify which configuration options to import.

4. Specify the path and filename of the XML file to import. Click on **OK** to proceed with the import.


GFI ReportCenter
Import process completed successfully. In order to see the warnings that occurred during import, please click on the Details button.
Details:
Importing RC Scheduling settings.
Importing settings for GFI LANguard 9.0 ReportPack.
Importing custom reports.
Importing scheduled reports.
Importing favorite reports.
Importing connection string.
OK
Details

Screenshot 46 – Import configuration success


GFI ReportCenter
Importing from C:\Program Files\Common Files\GFI\ReportCenter\Framework v3.5\SavedReports\Omar.xml file completed successfully. Note that some of the settings could be only partially imported. Please see the debug logs for more details.
Please close and restart GFI ReportCenter to load up with the imported items.
OK

Screenshot 47 - Import configuration success - restart notification

5. Close and restart GFI ReportCenter to activate the imported items.

7. General options

7.1 Viewing the product ReportPack version details

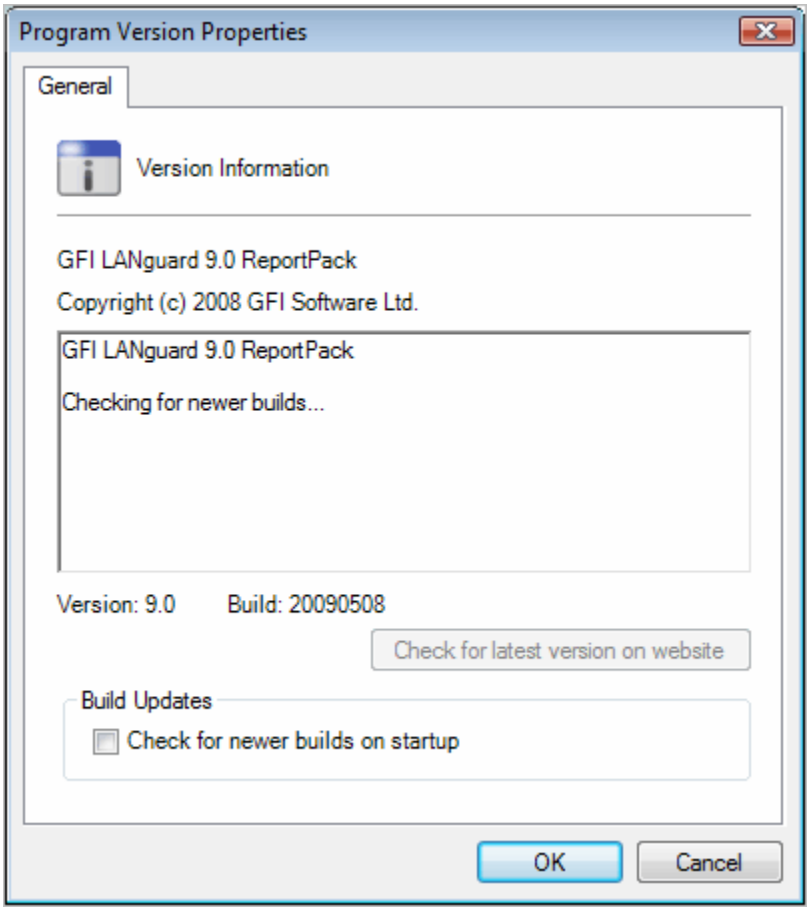
To view the version information of your product ReportPacks:

1. Select the product ReportPack from the **Product Selection** drop down list.

2. Click on the **Options** navigation button and select the **Version Information** node. The version details will be displayed in the right pane of the management console.

7.2 Checking the web for newer builds

Periodically GFI releases product and ReportPack updates which can be automatically downloaded from the GFI website. To check if a newer built is available for download:



Screenshot 48 - Version Properties: Check for newer builds dialog

1. Select the respective product (for example, GFI LANguard 9.0 Reports) from the **Product Selection** drop down list.

2. Click on the **Options** navigation button.

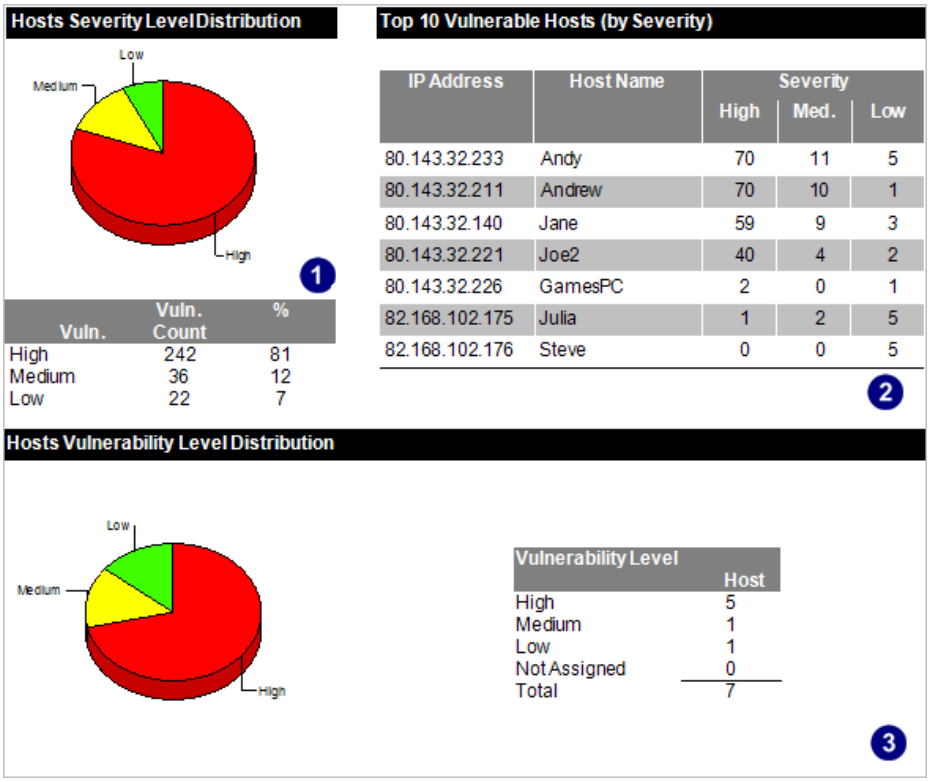
3. Right-click on the **Version Information** node and select **Checking for newer builds…**

NOTE: GFI LANguard 9.0 ReportPack is configured by default to check for newer builds on startup.

8. Appendix: GFI LANguard default reports

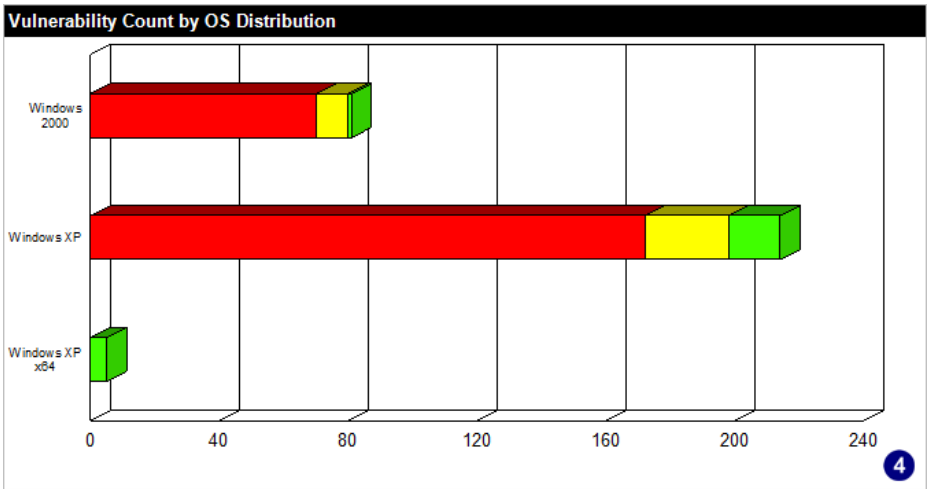
8.1 Vulnerability assessment reports

8.1.1 Network vulnerability summary



Screenshot 49 – Sample report showing network vulnerability summary

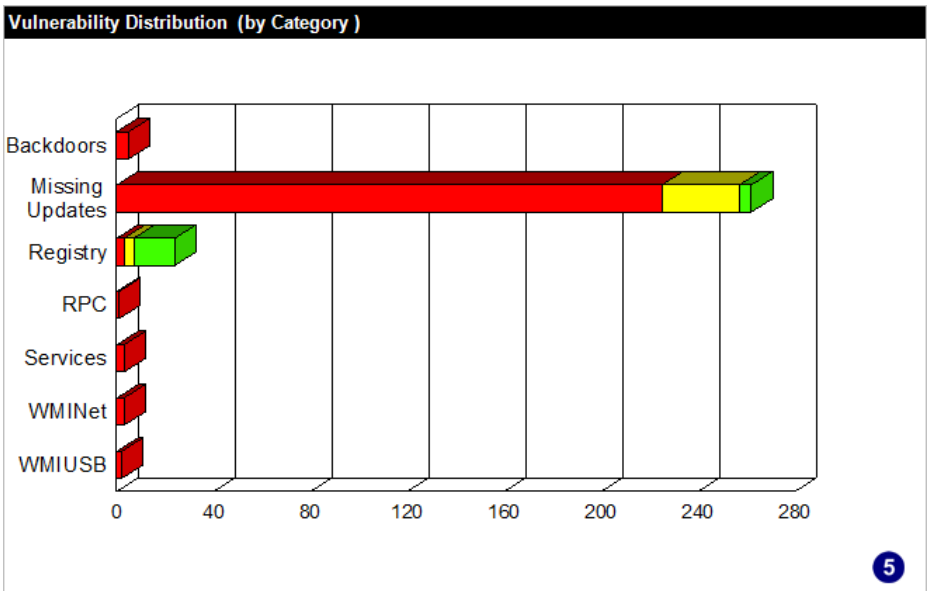
1	Chart displaying vulnerability severity distributions
2	List showing the top 10 most vulnerable host machines ordered by severity
3	Chart displaying vulnerability level distributions across host machines on the network



Operating System	Severity Distribution			
	Total	High	Med.	Low
Windows 2000	81	70	10	1
Windows XP	214	172	26	16
Windows XP x64	5	0	0	5

Screenshot 50 – Sample report showing network vulnerability summary

4	Chart displaying the vulnerability distribution for each operating system on the network

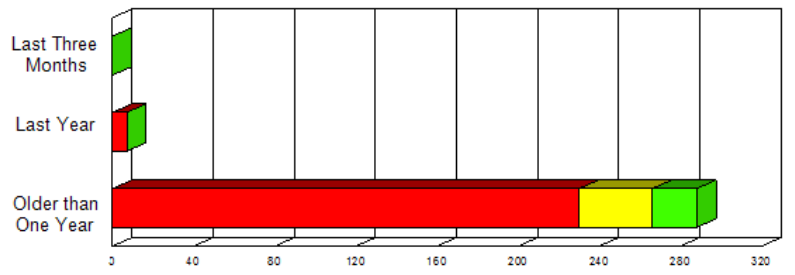


Vulnerability Category	Severity Distribution			
	Total	High	Med.	Low
Backdoors	5	5	0	0
Missing Updates	262	225	32	5
Registry	24	3	4	17
RPC	1	1	0	0
Services	3	3	0	0
WMINet	3	3	0	0
WMIUSB	2	2	0	0

Screenshot 51 – Sample report showing network vulnerability summary

5	Chart displaying vulnerability categories and their distribution

Vulnerability Distribution (by Timestamp)



Vulnerability Category	Severity Distribution			
	Total	High	Med.	Low
Last Three Months	0	0	0	0
Last Year	7	7	0	0
Older than One Year	288	230	36	22

Screenshot 52 – Sample report showing network vulnerability summary

6	Chart displaying the vulnerability distribution over time

Top 10 Most Common Vulnerabilities

Missing Update : Windows Malicious Software Removal Tool - January 2007 (KB890830)

7

Product	Timestamp	References	Type	Severity	Count
Windows	2007-01-09	N/A	Missing Update	High	5

Vulnerability : AutoShareWKS

Product	Timestamp	References	Type	Severity	Count
N/A	2002-01-01	N/A	Registry	Low	3

Missing Update : Security Update for Microsoft Data Access Components (KB832483)

Product	Timestamp	References	Type	Severity	Count
Windows	2005-02-17	N/A	Missing Update	High	3

Missing Update : Security Update for Windows Media Player Plug-in (KB911564)

Product	Timestamp	References	Type	Severity	Count
Windows	2006-02-14	N/A	Missing Update	High	3

Missing Update : Security Update for Windows XP (KB920685)

Product	Timestamp	References	Type	Severity	Count
Windows	2006-09-12	N/A	Missing Update	Medium	3

Missing Update : Security Update for Microsoft Windows (KB824105)

Product	Timestamp	References	Type	Severity	Count
Windows	2003-09-09	N/A	Missing Update	High	3

Missing Update : Security Update for Windows XP (KB912919)

Product	Timestamp	References	Type	Severity	Count
Windows	2006-01-05	N/A	Missing Update	High	2

Missing Update : Security Update for Windows XP (KB911927)

Product	Timestamp	References	Type	Severity	Count
Windows	2006-02-14	N/A	Missing Update	High	2

Top 10 Most Vulnerable Products

Product	Severity Distribution			
	Total	High	Med.	Low
Windows	262	225	32	5
Microsoft Windows NT	1	0	0	1

8

Screenshot 53 – Sample report showing network vulnerability summary

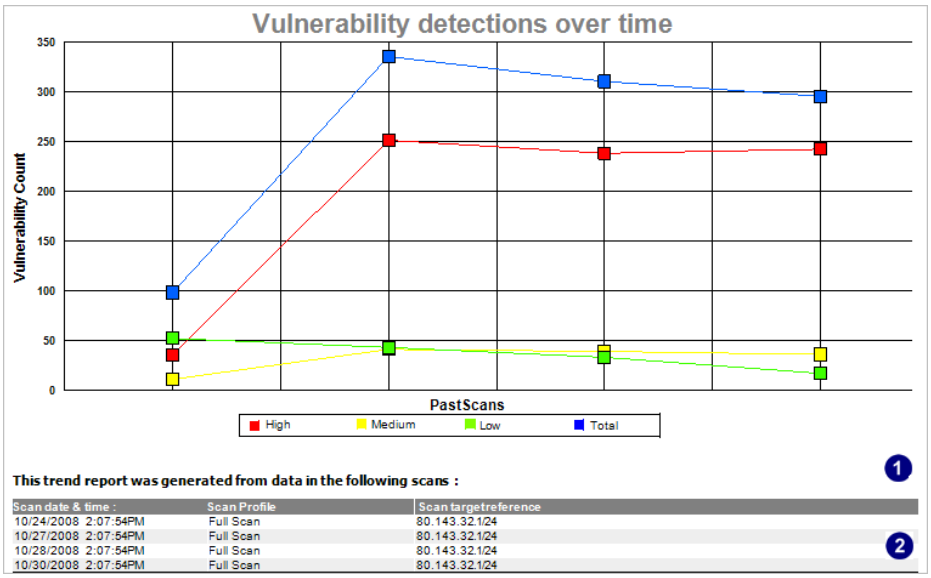
7	Chart displaying the 10 most common vulnerabilities
8	Chart displaying the 10 most vulnerable products

Use this report to:

- Display vulnerability counts for different categories

- Identify the 10 most vulnerable host machines
- Identify the 10 most vulnerable products
- Identify the 10 most common vulnerabilities.

8.1.2 Network vulnerability trend



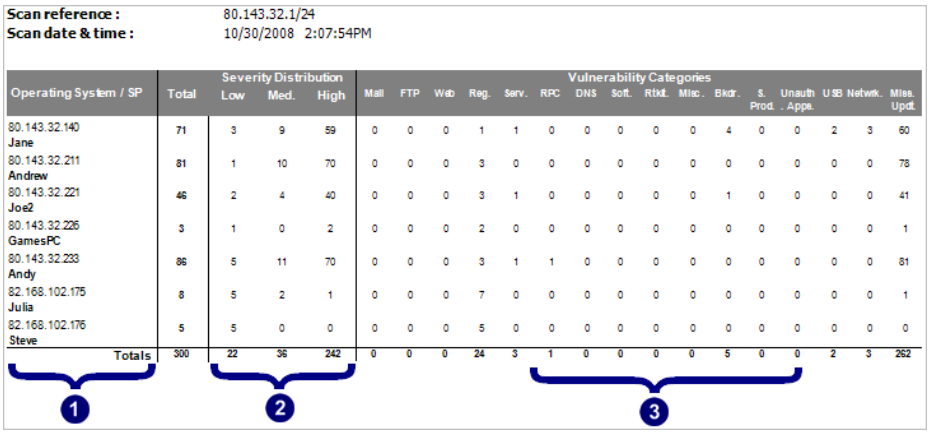
Screenshot 54 – Sample report showing network vulnerability trend

1	Chart displaying past scans and vulnerability totals for each scan
2	List of past scans and respective scan profiles

Use this report to:

- Graphically illustrate how the number of vulnerabilities on the network has changed over a given time span.

8.1.3 Vulnerability distribution by host



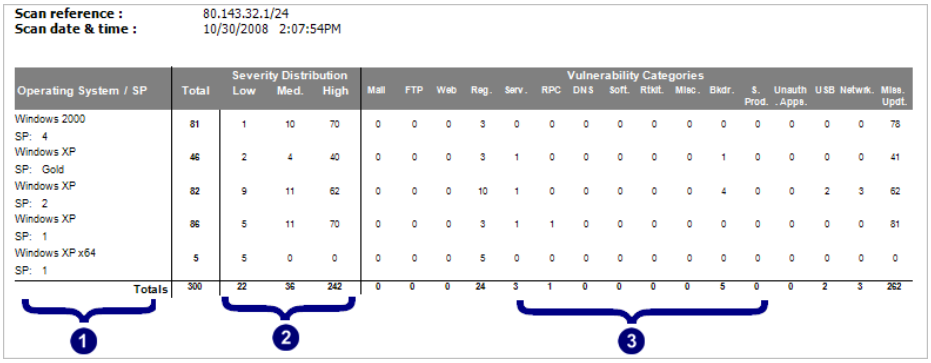
Screenshot 55 – Sample report showing vulnerability distribution by host

1	List of IP addresses and host names on which vulnerabilities were detected
2	The number of low, medium and high severity vulnerabilities detected on each host
3	The number of vulnerabilities detected on each host distributed by vulnerability category

Use this report to:

- Generate statistics showing vulnerability counts for each host machine.

8.1.4 Vulnerability distribution by operating system



Scan reference : 80.143.32.1/24
Scan date & time : 10/30/2008 2:07:54PM

Operating System / SP	Severity Distribution				Vulnerability Categories															
	Total	Low	Med.	High	Mail	FTP	Web	Reg.	Serv.	RPC	DNS	Soft.	Rtkit.	Misc.	Bkdr.	S. Prod.	Unauth. Apps.	USB	Netwrk.	Miss. Updt.
Windows 2000 SP: 4	81	1	10	70	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	78
Windows XP SP: Gold	46	2	4	40	0	0	0	3	1	0	0	0	0	0	1	0	0	0	0	41
Windows XP SP: 2	82	9	11	62	0	0	0	10	1	0	0	0	0	0	4	0	0	2	3	62
Windows XP SP: 1	86	5	11	70	0	0	0	3	1	1	0	0	0	0	0	0	0	0	0	81
Windows XP x64 SP: 1	5	5	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0
Totals	300	22	36	242	0	0	0	24	3	1	0	0	0	0	5	0	0	2	3	262

1 2 3

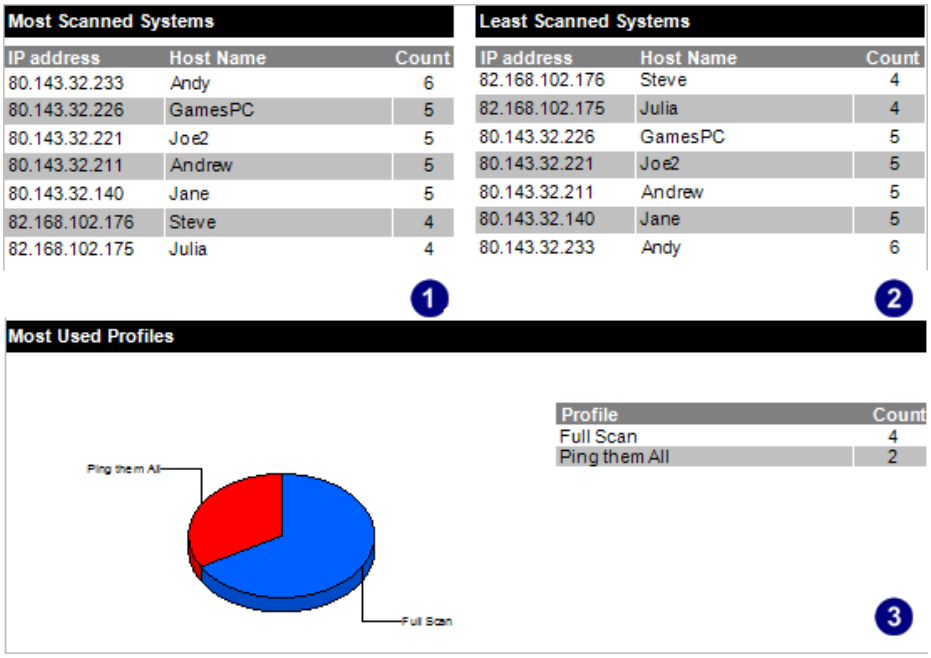
Screenshot 56 – Sample report showing vulnerability distribution by operating system

1	List of operating systems and service packs affected by one or more vulnerabilities
2	The number of low, medium and high severity vulnerabilities detected on each operating system
3	The number of vulnerabilities detected on each operating system distributed by vulnerability category

Use this report to:

- Generate statistics showing vulnerability counts for each operating system.

8.1.5 Security scans history



Most Scanned Systems

IP address	Host Name	Count
80.143.32.233	Andy	6
80.143.32.226	GamesPC	5
80.143.32.221	Joe2	5
80.143.32.211	Andrew	5
80.143.32.140	Jane	5
82.168.102.176	Steve	4
82.168.102.175	Julia	4

Least Scanned Systems

IP address	Host Name	Count
82.168.102.176	Steve	4
82.168.102.175	Julia	4
80.143.32.226	GamesPC	5
80.143.32.221	Joe2	5
80.143.32.211	Andrew	5
80.143.32.140	Jane	5
80.143.32.233	Andy	6

1 2

Most Used Profiles

Profile	Count
Full Scan	4
Ping them All	2

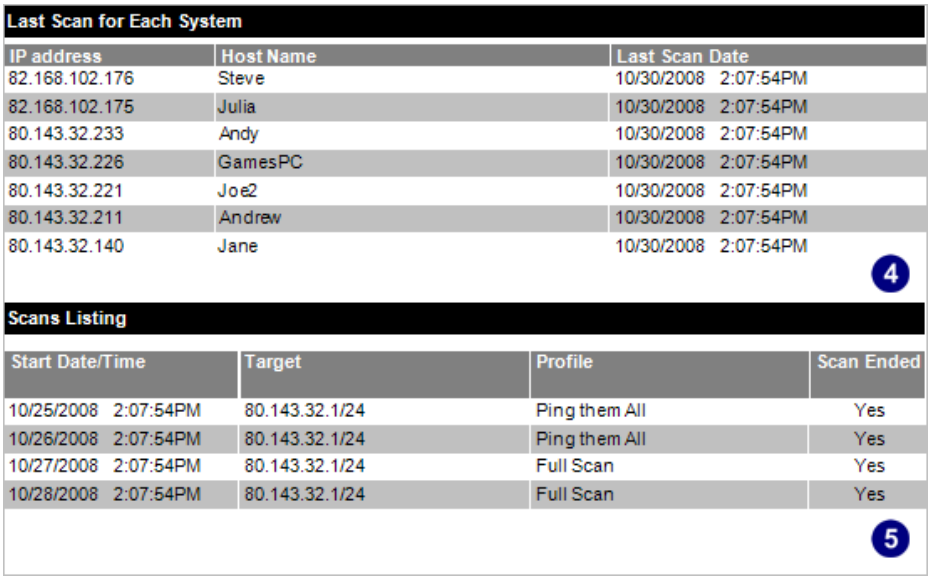
Ping them All
Full Scan

3

Screenshot 57 – Sample report showing security scans history

1	List showing the host machines with the highest number of scans and the respective scan count
2	List showing the host machines with the lowest number of scans and the

	respective scan count
3	Chart displaying scan profile usage



Last Scan for Each System

IP address	Host Name	Last Scan Date
82.168.102.176	Steve	10/30/2008 2:07:54PM
82.168.102.175	Julia	10/30/2008 2:07:54PM
80.143.32.233	Andy	10/30/2008 2:07:54PM
80.143.32.226	GamesPC	10/30/2008 2:07:54PM
80.143.32.221	Joe2	10/30/2008 2:07:54PM
80.143.32.211	Andrew	10/30/2008 2:07:54PM
80.143.32.140	Jane	10/30/2008 2:07:54PM

4

Scans Listing

Start Date/Time	Target	Profile	Scan Ended
10/25/2008 2:07:54PM	80.143.32.1/24	Ping them All	Yes
10/26/2008 2:07:54PM	80.143.32.1/24	Ping them All	Yes
10/27/2008 2:07:54PM	80.143.32.1/24	Full Scan	Yes
10/28/2008 2:07:54PM	80.143.32.1/24	Full Scan	Yes

5

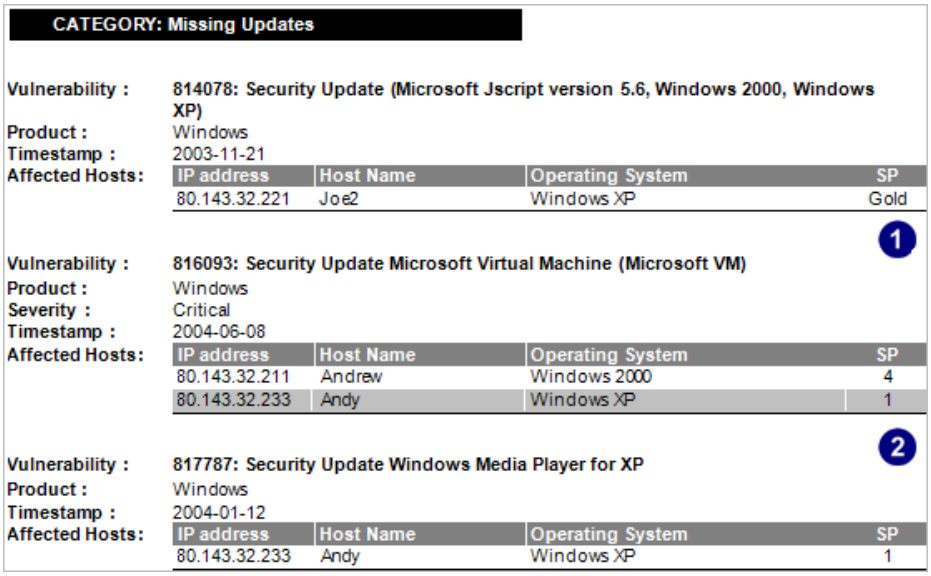
Screenshot 58 – Sample report showing security scans history

4	List showing date and time of the last scan performed on each host
5	List showing all scans performed

Use this report to:

- Display information and statistics on all network security scans performed.

8.1.6 Vulnerability listing by category



CATEGORY: Missing Updates

Vulnerability : 814078: Security Update (Microsoft Jscript version 5.6, Windows 2000, Windows XP)
Product : Windows
Timestamp : 2003-11-21
Affected Hosts:

IP address	Host Name	Operating System	SP
80.143.32.221	Joe2	Windows XP	Gold

1

Vulnerability : 816093: Security Update Microsoft Virtual Machine (Microsoft VM)
Product : Windows
Severity : Critical
Timestamp : 2004-06-08
Affected Hosts:

IP address	Host Name	Operating System	SP
80.143.32.211	Andrew	Windows 2000	4
80.143.32.233	Andy	Windows XP	1

2

Vulnerability : 817787: Security Update Windows Media Player for XP
Product : Windows
Timestamp : 2004-01-12
Affected Hosts:

IP address	Host Name	Operating System	SP
80.143.32.233	Andy	Windows XP	1

Screenshot 59 – Sample report showing vulnerability listing by category

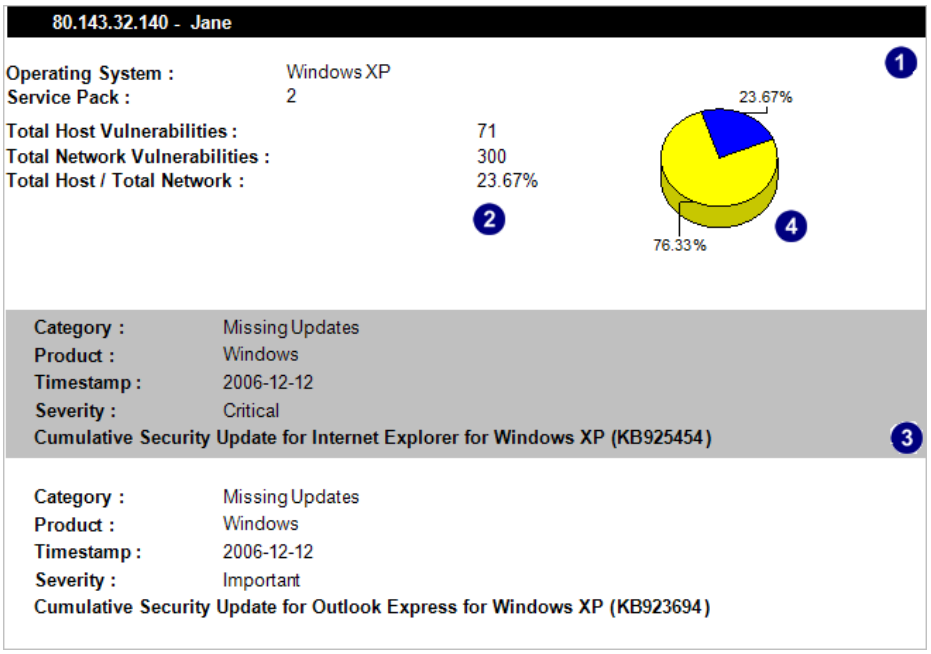
1	Vulnerability details including name, description and severity

2	List of host machines affected by each vulnerability detected

Use this report to:

- List detected vulnerabilities grouped by category, and the host machines affected by each vulnerability.

8.1.7 Vulnerability listing by host



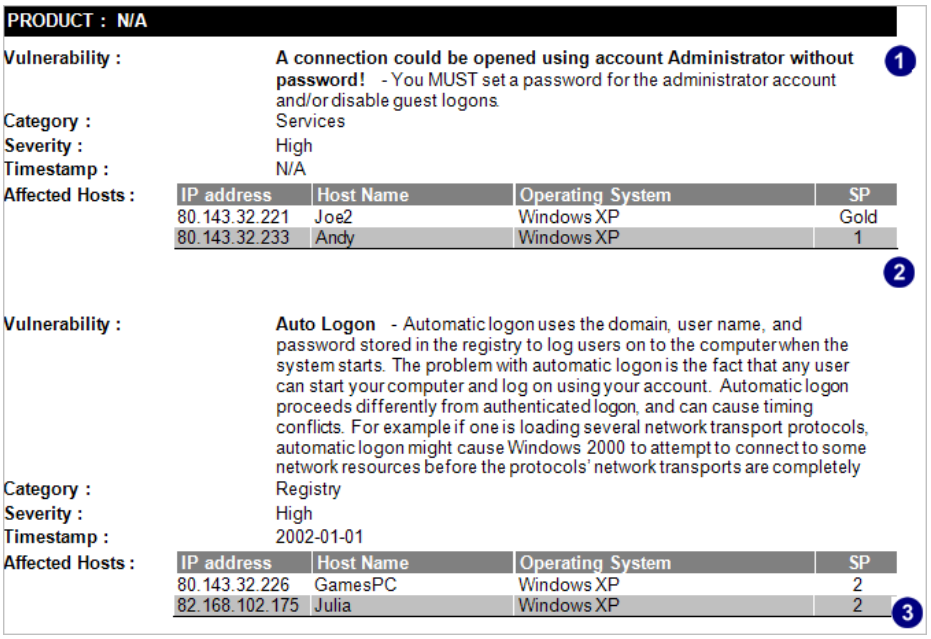
Screenshot 60 – Sample report showing vulnerability listing by host

1	Host machine details on which vulnerabilities were detected
2	Vulnerability count for each host, also shown as a percentage of total vulnerabilities detected on the network
3	List of vulnerability details for each host, including name, description and severity
4	Chart displaying percentage of vulnerabilities detected on each host compared to total vulnerabilities detected on the network

Use this report to:

- List the vulnerabilities detected for each host machine on the network.

8.1.8 Vulnerability listing by product


PRODUCT : N/A
Vulnerability :
A connection could be opened using account Administrator without password! - You MUST set a password for the administrator account and/or disable guest logons.
Category : Services
Severity : High
Timestamp : N/A
Affected Hosts :
IP address | Host Name | Operating System | SP
80.143.32.221 | Joe2 | Windows XP | Gold
80.143.32.233 | Andy | Windows XP | 1
Vulnerability :
Auto Logon - Automatic logon uses the domain, user name, and password stored in the registry to log users on to the computer when the system starts. The problem with automatic logon is the fact that any user can start your computer and log on using your account. Automatic logon proceeds differently from authenticated logon, and can cause timing conflicts. For example if one is loading several network transport protocols, automatic logon might cause Windows 2000 to attempt to connect to some network resources before the protocols' network transports are completely
Category : Registry
Severity : High
Timestamp : 2002-01-01
Affected Hosts :
IP address | Host Name | Operating System | SP
80.143.32.226 | GamesPC | Windows XP | 2
82.168.102.175 | Julia | Windows XP | 2
1
2
3

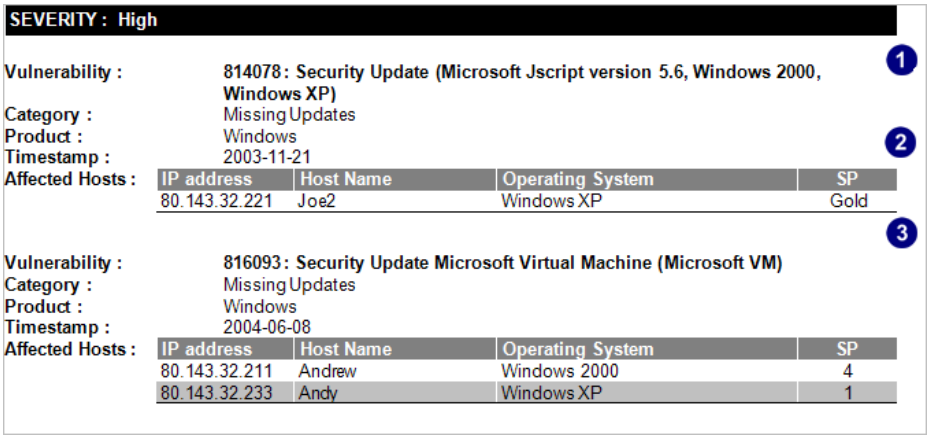
Screenshot 61 – Sample report showing vulnerability listing by product

1	Name of product for which vulnerabilities were detected
2	Vulnerability details for each product, including name, description and severity
3	List of host machines affected by each product vulnerability detected

Use this report to:

- List detected vulnerabilities grouped by product, and the host machines affected by each vulnerability.

8.1.9 Vulnerability listing by severity


SEVERITY : High
Vulnerability :
814078 : Security Update (Microsoft Jscript version 5.6, Windows 2000, Windows XP)
Category : Missing Updates
Product : Windows
Timestamp : 2003-11-21
Affected Hosts :
IP address | Host Name | Operating System | SP
80.143.32.221 | Joe2 | Windows XP | Gold
Vulnerability :
816093 : Security Update Microsoft Virtual Machine (Microsoft VM)
Category : Missing Updates
Product : Windows
Timestamp : 2004-06-08
Affected Hosts :
IP address | Host Name | Operating System | SP
80.143.32.211 | Andrew | Windows 2000 | 4
80.143.32.233 | Andy | Windows XP | 1
1
2
3

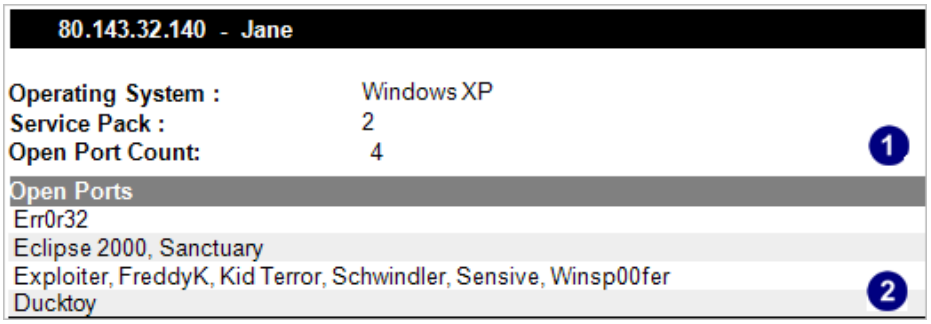
Screenshot 62 – Sample report showing vulnerability listing by severity

1	Severity level
2	Vulnerability details for each severity level, including name and description
3	List of host machines affected by vulnerabilities detected for each security level

Use this report to:

- List detected vulnerabilities grouped by severity, and the host machines affected by each vulnerability.

8.1.10 Open Trojan ports by host



Screenshot 63 – Sample report showing open Trojan ports by cost

1	Details of host machines having open ports associated with Trojans
2	List of open ports for each host and the names of Trojans targeting each port

Use this report to:

- List open ports, grouped by host machine, which could potentially serve as a backdoor for Trojans.

8.1.11 Open Trojan ports

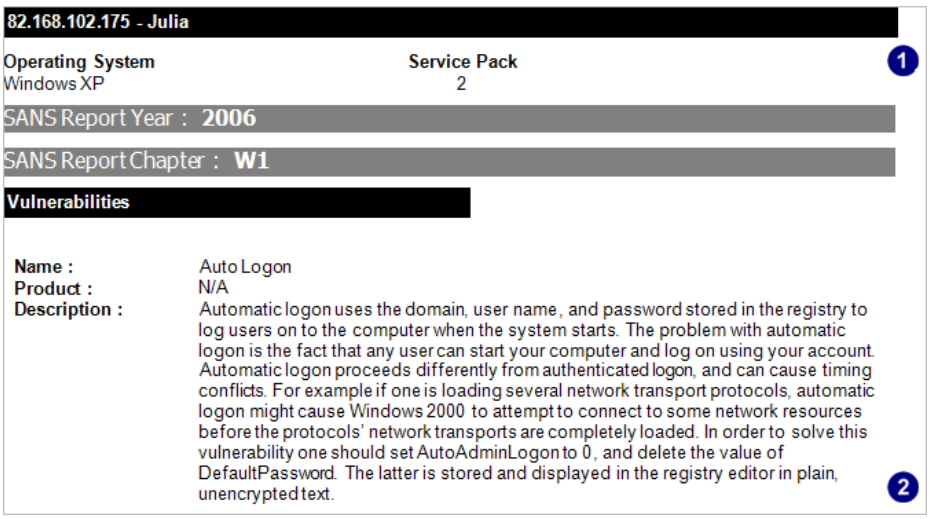
Screenshot 64 – Sample report showing open Trojan ports

1	List showing the most common open Trojan ports detected on the network

Use this report to:

- List the 20 most common open ports found on the network, which could potentially serve as a backdoor for Trojans.

8.1.12 Top SANS vulnerabilities status


82.168.102.175 - Julia
Operating System
Windows XP
Service Pack
2
1
SANS Report Year : 2006
SANS Report Chapter : W1
Vulnerabilities
Name :
Auto Logon
Product :
N/A
Description :
Automatic logon uses the domain, user name, and password stored in the registry to log users on to the computer when the system starts. The problem with automatic logon is the fact that any user can start your computer and log on using your account. Automatic logon proceeds differently from authenticated logon, and can cause timing conflicts. For example if one is loading several network transport protocols, automatic logon might cause Windows 2000 to attempt to connect to some network resources before the protocols' network transports are completely loaded. In order to solve this vulnerability one should set AutoAdminLogon to 0, and delete the value of DefaultPassword. The latter is stored and displayed in the registry editor in plain, unencrypted text.
2

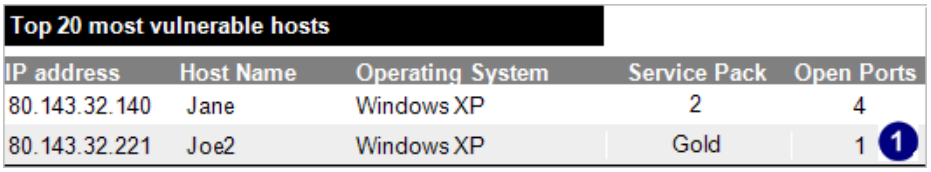
Screenshot 65 – Sample report showing top SANS vulnerabilities status

1	Host machine details on which vulnerabilities reported by SANS were detected
2	List showing SANS vulnerability details, including name, description and product affected. SANS vulnerabilities are grouped by year and chapter

Use this report to:

- List the vulnerabilities detected for each host machine, based on the SANS top-20 report of vulnerabilities.

8.1.13 Vulnerable hosts based on open ports



Top 20 most vulnerable hosts

IP address	Host Name	Operating System	Service Pack	Open Ports
80.143.32.140	Jane	Windows XP	2	4
80.143.32.221	Joe2	Windows XP	Gold	1

1

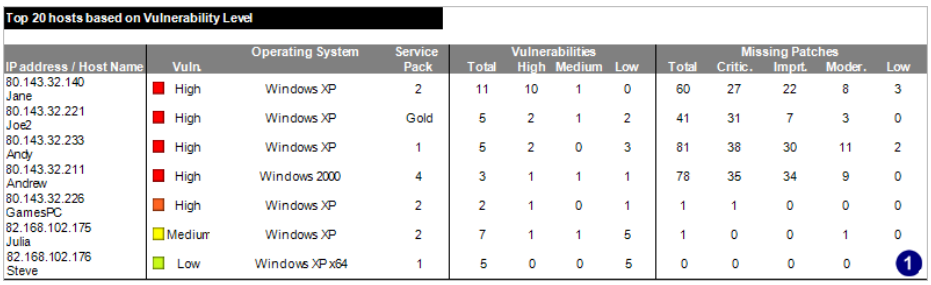
Screenshot 66 – Sample report showing vulnerable hosts based on open ports

1	List showing the top 20 host machines most likely to be compromised by Trojans

Use this report to:

- List the 20 most vulnerable host machines, based on the number of open Trojan ports found.

8.1.14 Vulnerable hosts based on vulnerability level



Top 20 hosts based on Vulnerability Level

IP address / Host Name	Vuln.	Operating System	Service Pack	Vulnerabilities Total	High	Medium	Low	Missing Patches Total	Critic.	Imprt.	Moder.	Low
80.143.32.140 Jane	High	Windows XP	2	11	10	1	0	60	27	22	8	3
80.143.32.221 Joe2	High	Windows XP	Gold	5	2	1	2	41	31	7	3	0
80.143.32.233 Andy	High	Windows XP	1	5	2	0	3	81	38	30	11	2
80.143.32.211 Andrew	High	Windows 2000	4	3	1	1	1	78	35	34	9	0
80.143.32.226 GamesPC	High	Windows XP	2	2	1	0	1	1	1	0	0	0
82.168.102.175 Julia	Mediurr	Windows XP	2	7	1	1	5	1	0	0	1	0
82.168.102.176 Steve	Low	Windows XP x64	1	5	0	0	5	0	0	0	0	1

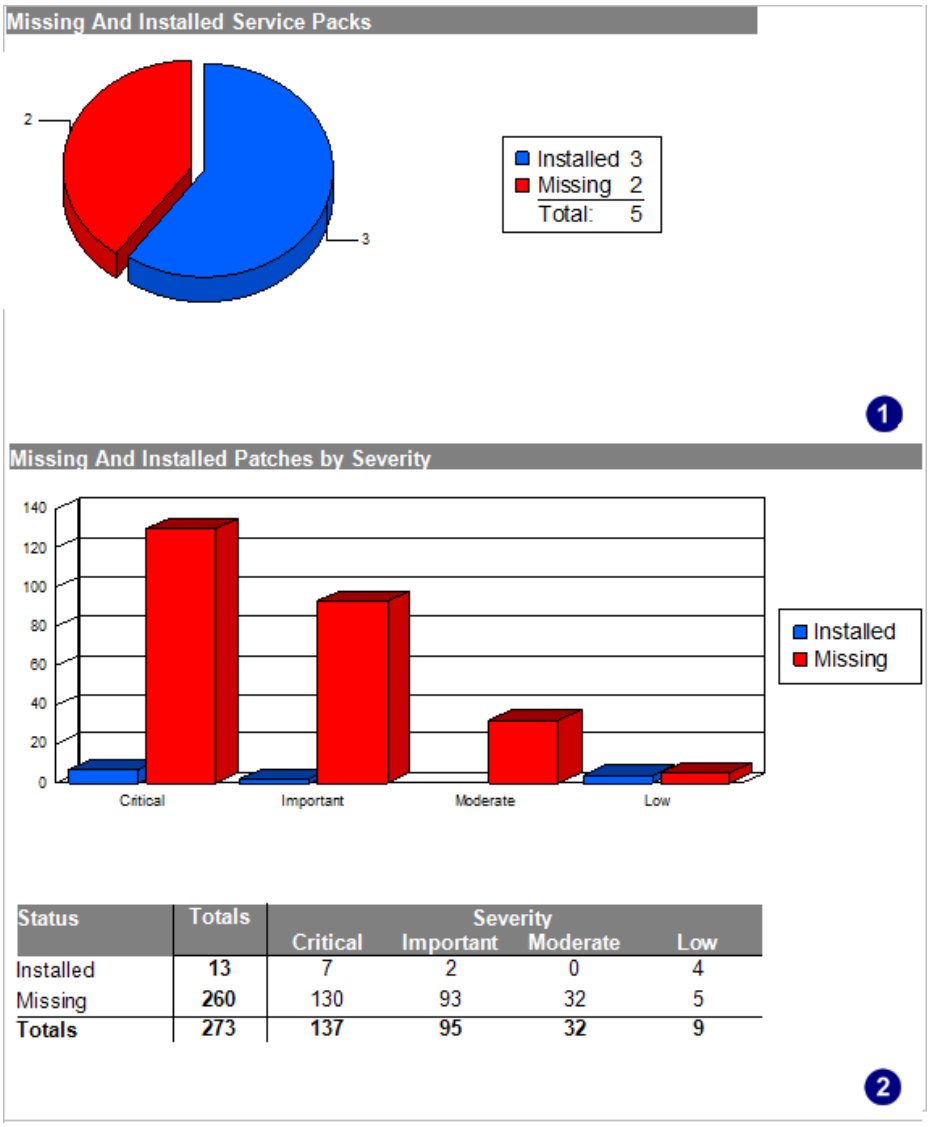
Screenshot 67 – Sample report showing vulnerable hosts based on vulnerability level

1	Host machine details showing the number of vulnerabilities and missing patches detected according to criticality

Use this report to:

- List the 20 most vulnerable host machines for each network security scan, based on vulnerability level.

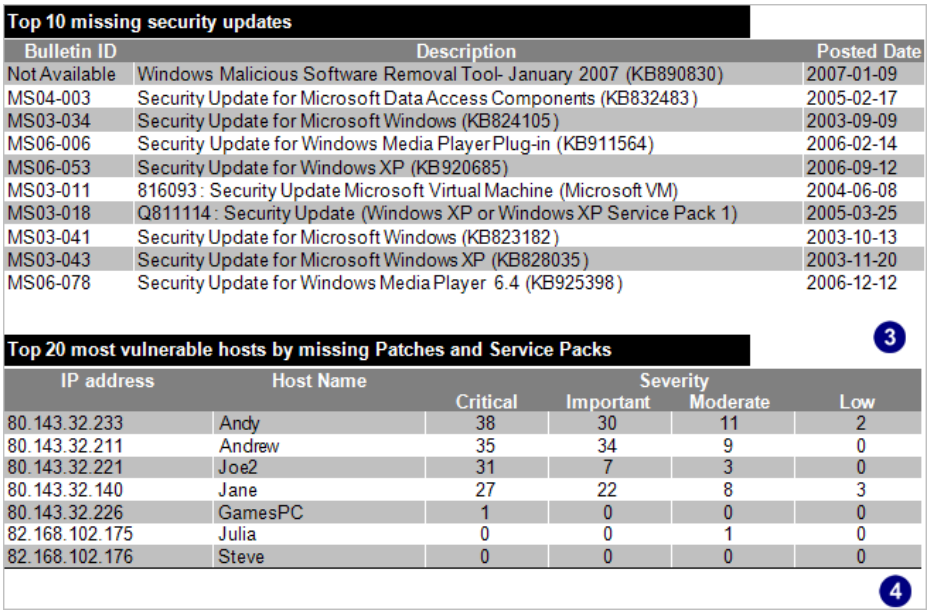
8.1.15 Network patching status



Status	Totals	Severity			
		Critical	Important	Moderate	Low
Installed	13	7	2	0	4
Missing	260	130	93	32	5
Totals	273	137	95	32	9

Screenshot 68 – Sample report showing network patching status

1	Chart displaying the number of installed and missing service packs
2	Chart displaying the number of installed and missing patches, grouped by severity



Top 10 missing security updates

Bulletin ID	Description	Posted Date
Not Available	Windows Malicious Software Removal Tool- January 2007 (KB890830)	2007-01-09
MS04-003	Security Update for Microsoft Data Access Components (KB832483)	2005-02-17
MS03-034	Security Update for Microsoft Windows (KB824105)	2003-09-09
MS06-006	Security Update for Windows Media Player Plug-in (KB911564)	2006-02-14
MS06-053	Security Update for Windows XP (KB920685)	2006-09-12
MS03-011	816093 : Security Update Microsoft Virtual Machine (Microsoft VM)	2004-06-08
MS03-018	Q811114 : Security Update (Windows XP or Windows XP Service Pack 1)	2005-03-25
MS03-041	Security Update for Microsoft Windows (KB823182)	2003-10-13
MS03-043	Security Update for Microsoft Windows XP (KB828035)	2003-11-20
MS06-078	Security Update for Windows Media Player 6.4 (KB925398)	2006-12-12

3

Top 20 most vulnerable hosts by missing Patches and Service Packs

IP address	Host Name	Severity			
		Critical	Important	Moderate	Low
80.143.32.233	Andy	38	30	11	2
80.143.32.211	Andrew	35	34	9	0
80.143.32.221	Joe2	31	7	3	0
80.143.32.140	Jane	27	22	8	3
80.143.32.226	GamesPC	1	0	0	0
82.168.102.175	Julia	0	0	1	0
82.168.102.176	Steve	0	0	0	0

4

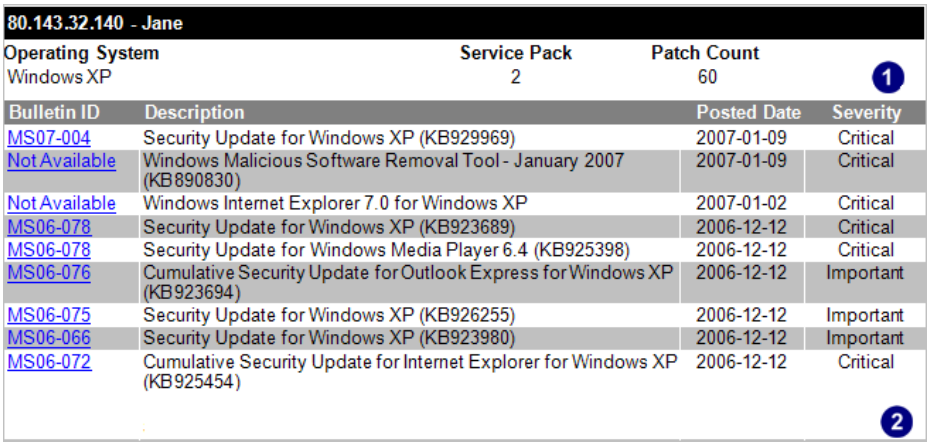
Screenshot 69 – Sample report showing network patching status

3	List showing the top 10 missing security updates
4	List showing the top 20 most vulnerable host machines, as a result of missing patches and service packs. The number of vulnerabilities detected is split according to severity

Use this report to:

- Illustrate the status of patches and service packs for host machines on the network.

8.1.16 Missing patches grouped by host



80.143.32.140 - Jane

Operating System	Service Pack	Patch Count
Windows XP	2	60

1

Bulletin ID	Description	Posted Date	Severity
MS07-004	Security Update for Windows XP (KB929969)	2007-01-09	Critical
Not Available	Windows Malicious Software Removal Tool - January 2007 (KB890830)	2007-01-09	Critical
Not Available	Windows Internet Explorer 7.0 for Windows XP	2007-01-02	Critical
MS06-078	Security Update for Windows XP (KB923689)	2006-12-12	Critical
MS06-078	Security Update for Windows Media Player 6.4 (KB925398)	2006-12-12	Critical
MS06-076	Cumulative Security Update for Outlook Express for Windows XP (KB923694)	2006-12-12	Important
MS06-075	Security Update for Windows XP (KB926255)	2006-12-12	Important
MS06-066	Security Update for Windows XP (KB923980)	2006-12-12	Important
MS06-072	Cumulative Security Update for Internet Explorer for Windows XP (KB925454)	2006-12-12	Critical

2

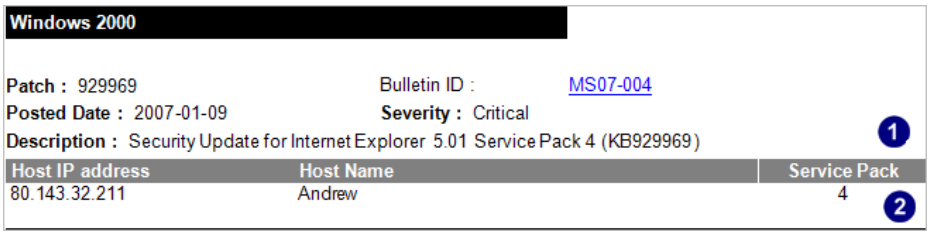
Screenshot 70 – Sample report showing missing patches grouped by host

1	Host machine details on which missing patches were detected
2	List of missing patch details for each host, including severity and URL link for further information

Use this report to:

- List missing patches grouped by host machine, including URL links providing further information on each missing patch.

8.1.17 Missing patches grouped by operating system



Windows 2000

Patch : 929969 **Bulletin ID :** MS07-004
Posted Date : 2007-01-09 **Severity :** Critical
Description : Security Update for Internet Explorer 5.01 Service Pack 4 (KB929969) (1)

Host IP address	Host Name	Service Pack
80.143.32.211	Andrew	4

(2)

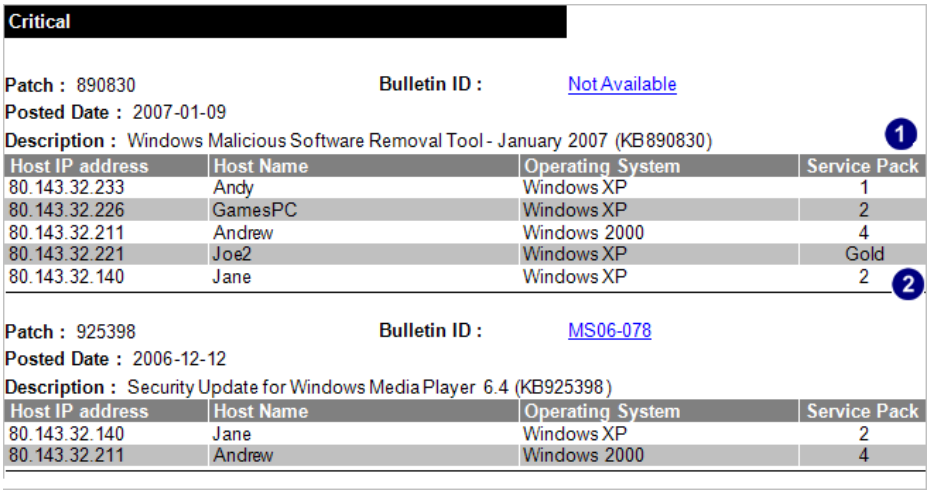
Screenshot 71 – Sample report showing missing patches grouped by operating system

1	Missing patch details for each operating system
2	List of host machines on which specific patches were found to be missing

Use this report to:

- List missing patches grouped by operating system, including the host machine names for each missing patch.

8.1.18 Missing patches grouped by severity



Critical

Patch : 890830 **Bulletin ID :** Not Available
Posted Date : 2007-01-09
Description : Windows Malicious Software Removal Tool - January 2007 (KB890830) (1)

Host IP address	Host Name	Operating System	Service Pack
80.143.32.233	Andy	Windows XP	1
80.143.32.226	GamesPC	Windows XP	2
80.143.32.211	Andrew	Windows 2000	4
80.143.32.221	Joe2	Windows XP	Gold
80.143.32.140	Jane	Windows XP	2

(2)

Patch : 925398 **Bulletin ID :** MS06-078
Posted Date : 2006-12-12
Description : Security Update for Windows Media Player 6.4 (KB925398)

Host IP address	Host Name	Operating System	Service Pack
80.143.32.140	Jane	Windows XP	2
80.143.32.211	Andrew	Windows 2000	4

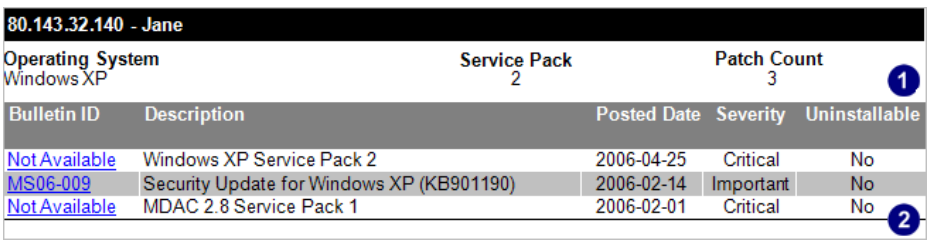
Screenshot 72 – Sample report showing missing patches grouped by severity

1	Missing patch details for each severity level
2	List of host machines on which specific patches were found to be missing

Use this report to:

- List missing patches grouped by severity, including the host machine names for each missing patch.

8.1.19 Installed patches grouped by host



80.143.32.140 - Jane

Operating System	Service Pack	Patch Count
Windows XP	2	3

(1)

Bulletin ID	Description	Posted Date	Severity	Uninstallable
Not Available	Windows XP Service Pack 2	2006-04-25	Critical	No
MS06-009	Security Update for Windows XP (KB901190)	2006-02-14	Important	No
Not Available	MDAC 2.8 Service Pack 1	2006-02-01	Critical	No

(2)

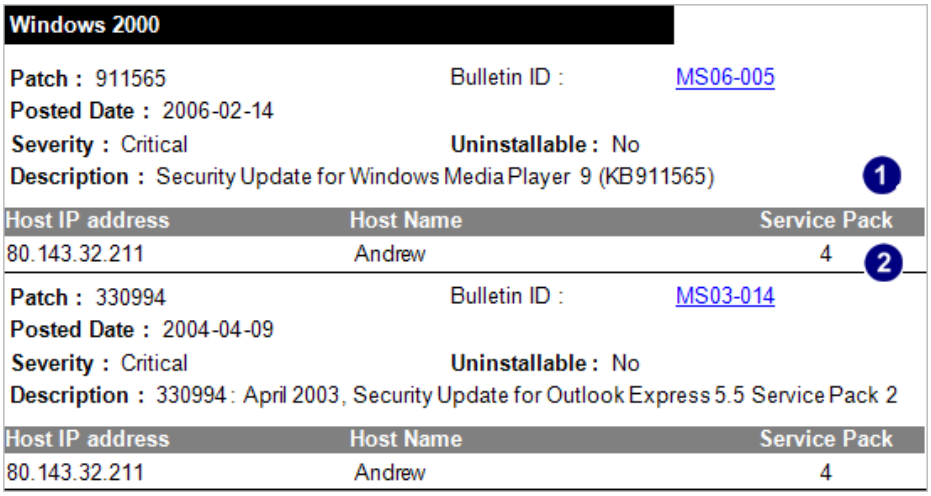
Screenshot 73 – Sample report showing installed patches grouped by host

1	Host machine details on which installed patches were detected
2	List of installed patch details for each host, including severity, URL link for further information and indication if the patch can be uninstalled

Use this report to:

- List installed patches grouped by host machine, including URL links providing further information on each installed patch.

8.1.20 Installed patches grouped by operating system



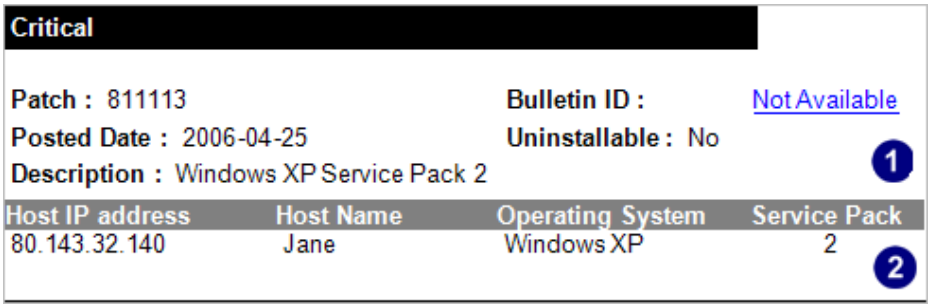
Screenshot 74 – Sample report showing installed patches grouped by operating system

1	Installed patch details for each operating system
2	List of host machines on which specific patches were found to be installed

Use this report to:

- List installed patches grouped by operating system, including the host machine names for each installed patch.

8.1.21 Installed patches grouped by severity



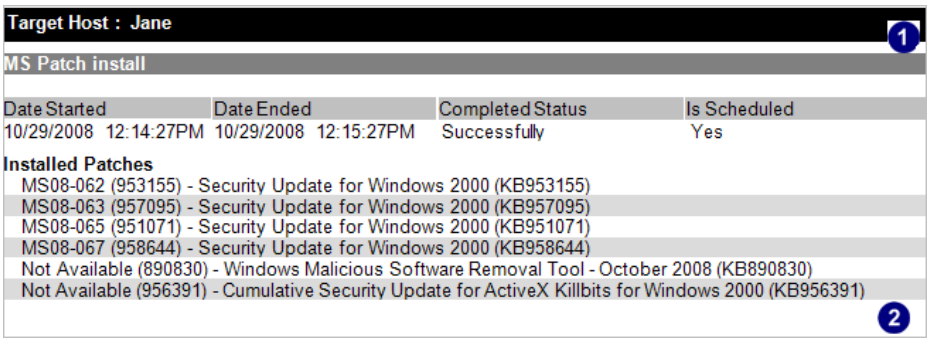
Screenshot 75 – Sample report showing installed patches grouped by severity

1	List of installed patches grouped by their severity level, including information on each patch
2	List of host machines on which specific patches were found to be installed

Use this report to:

- List installed patches grouped by severity, including the host machine names for each installed patch.

8.1.22 Remediation history by host


Target Host : Jane
1
MS Patch install
Date Started
Date Ended
Completed Status
Is Scheduled
10/29/2008 12:14:27PM
10/29/2008 12:15:27PM
Successfully
Yes
Installed Patches
MS08-062 (953155) - Security Update for Windows 2000 (KB953155)
MS08-063 (957095) - Security Update for Windows 2000 (KB957095)
MS08-065 (951071) - Security Update for Windows 2000 (KB951071)
MS08-067 (958644) - Security Update for Windows 2000 (KB958644)
Not Available (890830) - Windows Malicious Software Removal Tool - October 2008 (KB890830)
Not Available (956391) - Cumulative Security Update for ActiveX Killbits for Windows 2000 (KB956391)
2

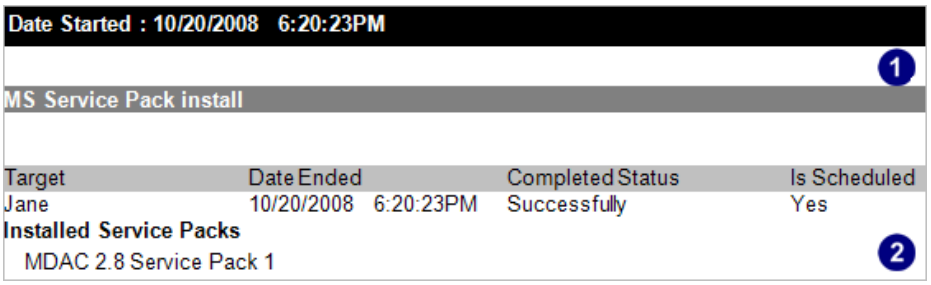
Screenshot 76 – Sample report showing deployment history by host

1	Host machine on which deployments were made
2	List of deployment details for each host, including file names deployed, and deployment status

Use this report to:

- Display patches deployment information grouped by host machine, including deployment details such as date and status.

8.1.23 Remediation history by date



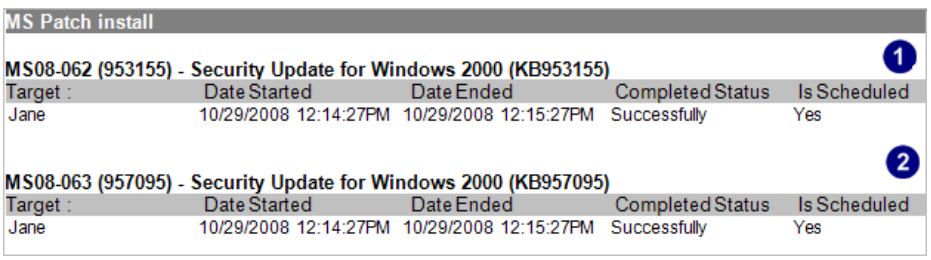
Screenshot 77 – Sample report showing deployment history by date

1	Deployment starting date
2	List of deployment details grouped by host, including file names deployed, and deployment status

Use this report to:

- Display patches deployment information by date and time, including details such as host machine names for each deployment.

8.1.24 Remediation history by patch/application



Screenshot 78 – Sample report showing deployment history by patch

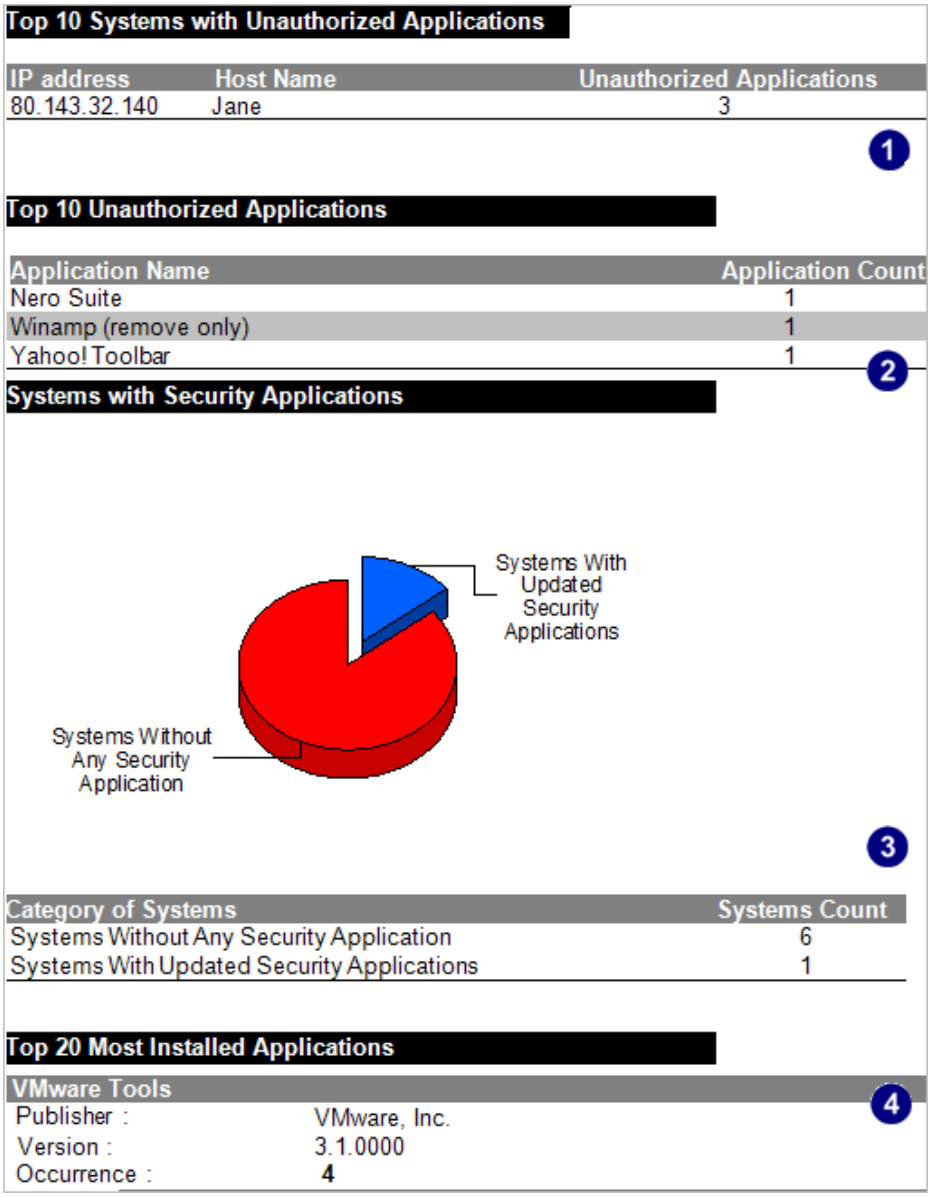
1	Name of patch deployed
2	List of host machines on which the patch was deployed and deployment details, including deployment status

Use this report to:

- Display patch deployment information grouped by patch applied, including details such as host machine names for each deployment.

8.2 Network and software audit reports

8.2.1 Software audit



Screenshot 79 – Sample report showing software audit

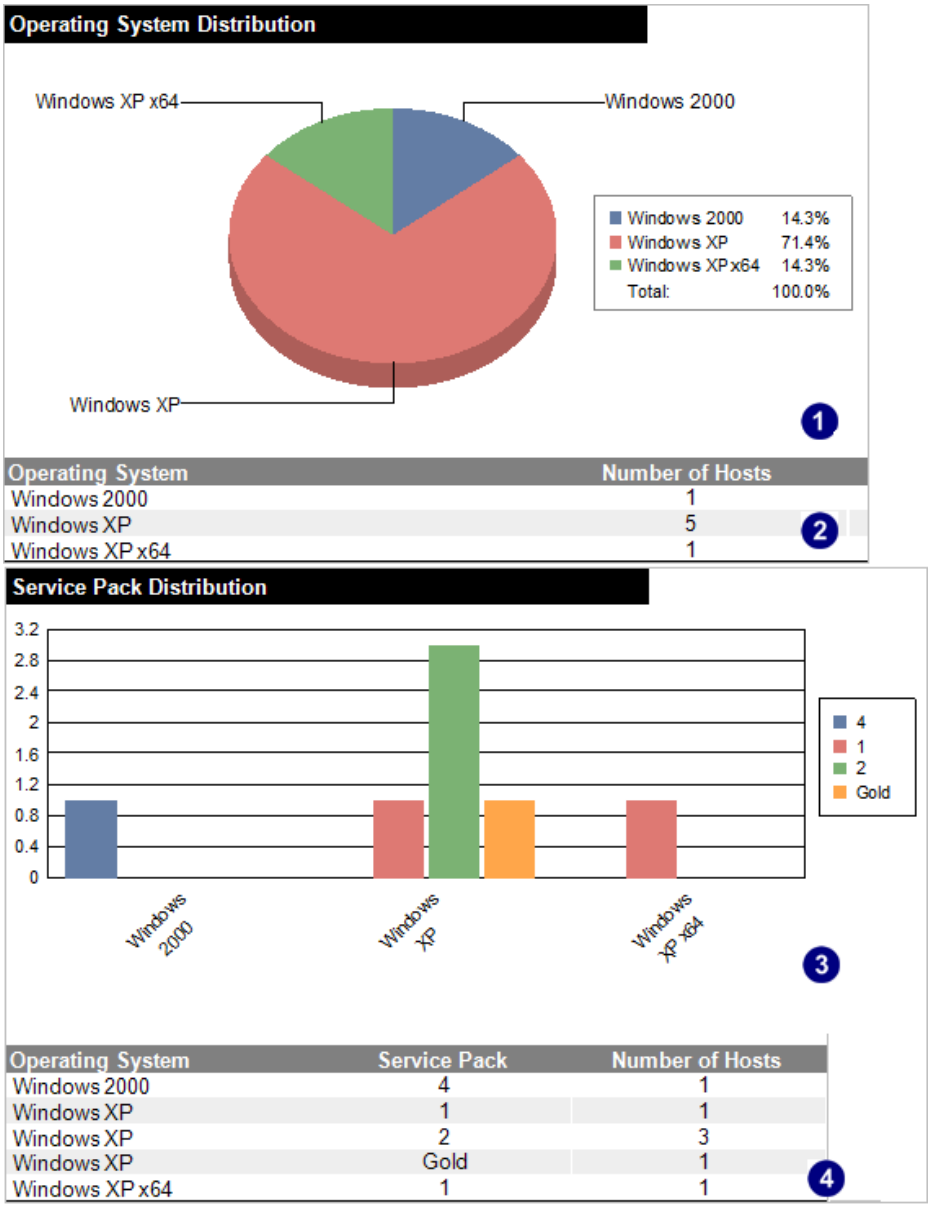
1	List showing the top 10 host machines with unauthorized applications
2	List showing the top 10 unauthorized applications

3	Chart displaying the status of security applications on host machines
4	List showing the top 20 installed applications

Use this report to:

- Identify unauthorized applications installed on host machines, detected during network security scans
- Identify the top 10 host machines with unauthorized applications
- Identify the top 10 unauthorized applications with highest number of installations
- Identify the top 20 installed applications
- Graphically represent the number of host machines without security applications, or with security applications not updated.

8.2.2 Operating system and service pack distribution



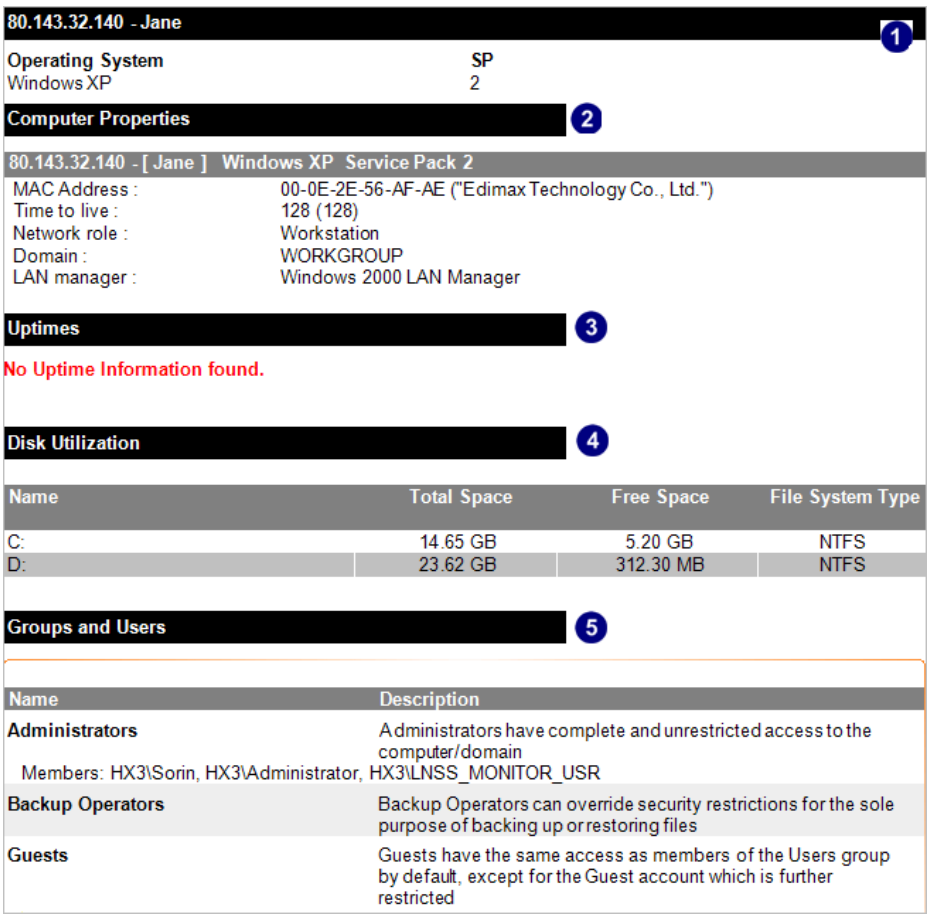
Screenshot 80 – Sample report showing operating system and service pack distribution

1	Chart displaying distribution percentage of each operating system on the network
2	List of operating systems, including the number of host machines on which they are installed
3	Chart displaying service pack distribution for each operating system
4	List of operating system service packs, including the number of host machines on which they are installed

Use this report to:

- Graphically represent operating systems detected on the network
- List the number of host machines for each operating system
- Graphically represent service packs detected on the network for each operating system
- List the number of host machines for each service pack installed.

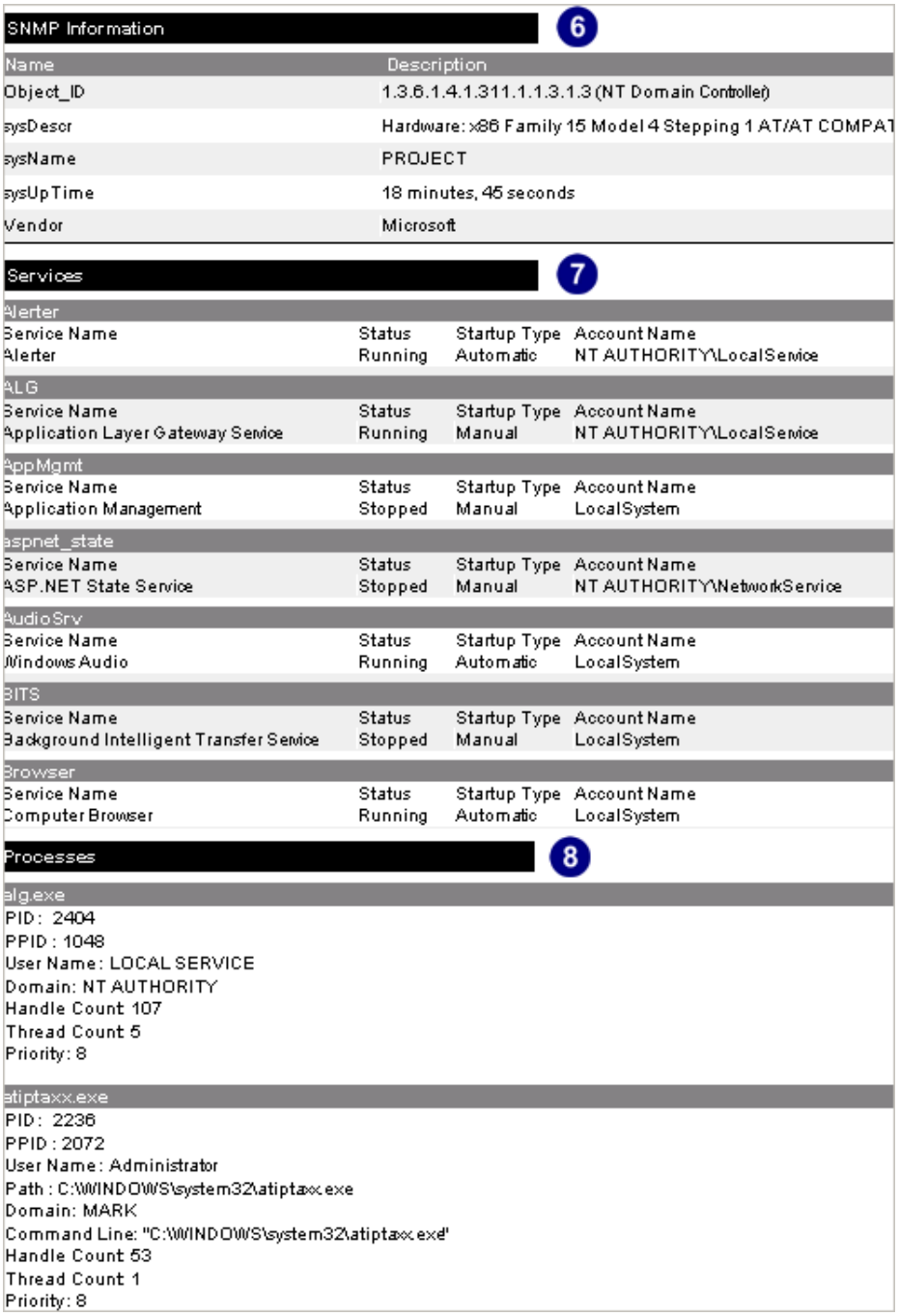
8.2.3 System information



Screenshot 81 – Sample report showing system information

1	Host machine IP and name
2	Host machine details, including MAC address and domain
3	Uptime details for each host machine, including time of day and uptime value
4	Disk utilization details for each host machine, including drive name, file system type, total storage space and free storage space

5	Group and user details for each host machine, including group name, group members, user privileges and user bad password count



SNMP Information 6

Name	Description
Object_ID	1.3.6.1.4.1.311.1.1.3.1.3 (NT Domain Controller)
sysDescr	Hardware: x86 Family 15 Model 4 Stepping 1 AT/AT COMPAT
sysName	PROJECT
sysUpTime	18 minutes, 45 seconds
Vendor	Microsoft

Services 7

Alerter

Service Name	Status	Startup Type	Account Name
Alerter	Running	Automatic	NT AUTHORITY\LocalService

ALG

Service Name	Status	Startup Type	Account Name
Application Layer Gateway Service	Running	Manual	NT AUTHORITY\LocalService

AppMgmt

Service Name	Status	Startup Type	Account Name
Application Management	Stopped	Manual	LocalSystem

aspnet_state

Service Name	Status	Startup Type	Account Name
ASP.NET State Service	Stopped	Manual	NT AUTHORITY\NetworkService

AudioSrv

Service Name	Status	Startup Type	Account Name
Windows Audio	Running	Automatic	LocalSystem

BITS

Service Name	Status	Startup Type	Account Name
Background Intelligent Transfer Service	Stopped	Manual	LocalSystem

Browser

Service Name	Status	Startup Type	Account Name
Computer Browser	Running	Automatic	LocalSystem

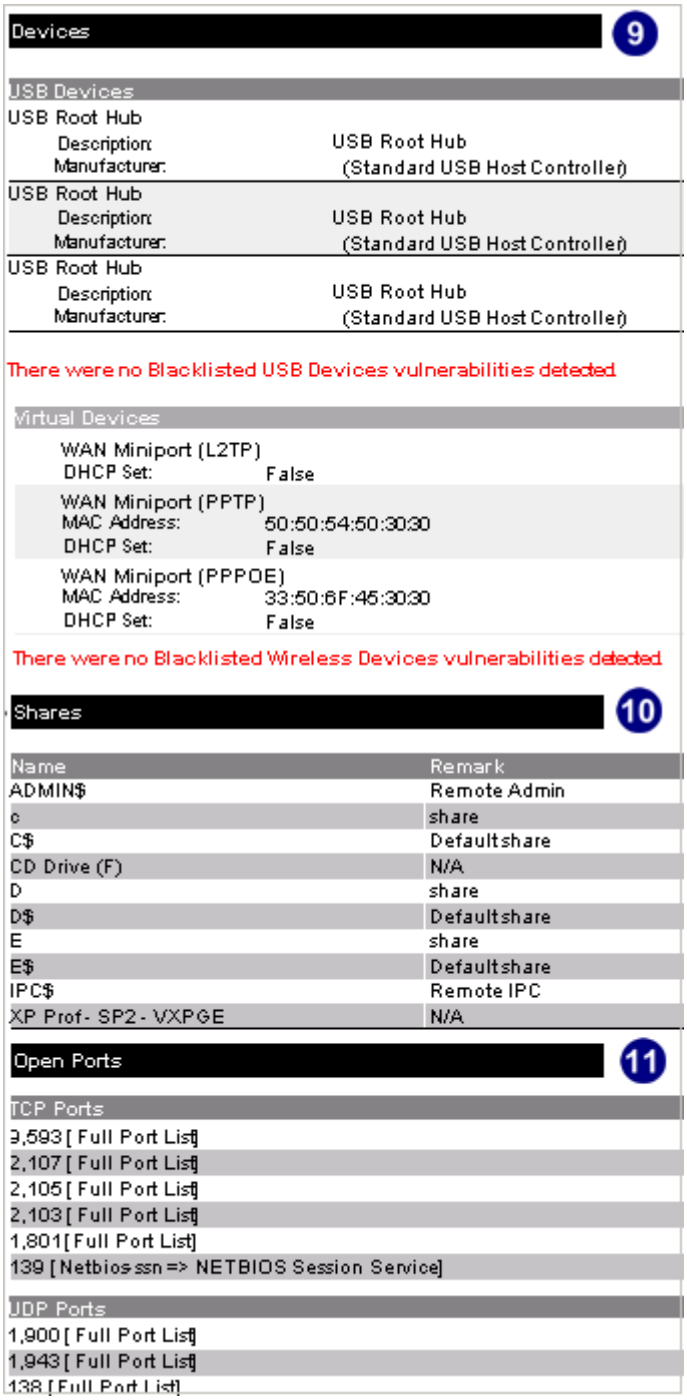
Processes 8

alg.exe
PID: 2404
PPID : 1048
User Name: LOCAL SERVICE
Domain: NT AUTHORITY
Handle Count: 107
Thread Count: 5
Priority: 8

atiptaxx.exe
PID: 2236
PPID : 2072
User Name: Administrator
Path : C:\WINDOWS\system32\atiptaxx.exe
Domain: MARK
Command Line: "C:\WINDOWS\system32\atiptaxx.exe"
Handle Count: 53
Thread Count: 1
Priority: 8

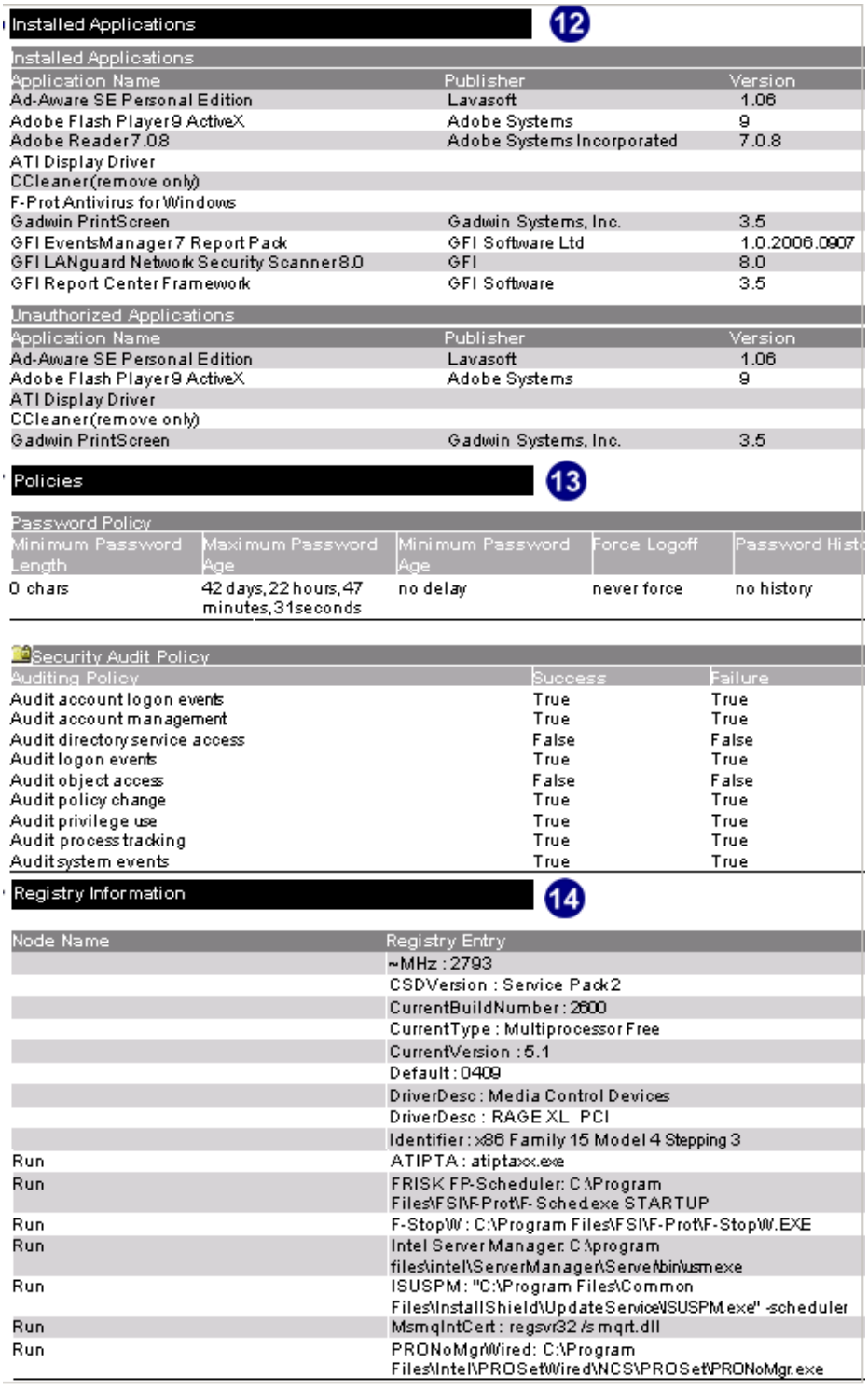
Screenshot 82 – Sample report showing system information

6	SNMP details for each host machine, including name and description
7	Service details for each host machine, including name, description, status, startup type and account name
8	Process details for each host machine, including process ID and account name



Screenshot 83 – Sample report showing system information

9	List showing USB devices, blacklisted USB devices, network cards and black listed wireless devices
10	Share folder details for each host machine, including name and remarks
11	Open port details for each host machine, including port number and name



Installed Applications 12

Installed Applications

Application Name	Publisher	Version
Ad-Aware SE Personal Edition	Lavasoft	1.06
Adobe Flash Player 9 ActiveX	Adobe Systems	9
Adobe Reader 7.0.8	Adobe Systems Incorporated	7.0.8
ATI Display Driver		
CCleaner (remove only)		
F-Prot Antivirus for Windows		
Gadwin PrintScreen	Gadwin Systems, Inc.	3.5
GFI EventsManager 7 Report Pack	GFI Software Ltd	1.0.2006.0907
GFI LANguard Network Security Scanner 8.0	GFI	8.0
GFI Report Center Framework	GFI Software	3.5

Unauthorized Applications

Application Name	Publisher	Version
Ad-Aware SE Personal Edition	Lavasoft	1.06
Adobe Flash Player 9 ActiveX	Adobe Systems	9
ATI Display Driver		
CCleaner (remove only)		
Gadwin PrintScreen	Gadwin Systems, Inc.	3.5

Policies 13

Password Policy

Minimum Password Length	Maximum Password Age	Minimum Password Age	Force Logoff	Password Histo
0 chars	42 days, 22 hours, 47 minutes, 31 seconds	no delay	never force	no history

Security Audit Policy

Auditing Policy	Success	Failure
Audit account logon events	True	True
Audit account management	True	True
Audit directory service access	False	False
Audit logon events	True	True
Audit object access	False	False
Audit policy change	True	True
Audit privilege use	True	True
Audit process tracking	True	True
Audit system events	True	True

Registry Information 14

Node Name	Registry Entry
	~MHz : 2793
	CSDVersion : Service Pack 2
	CurrentBuildNumber : 2600
	CurrentType : Multiprocessor Free
	CurrentVersion : 5.1
	Default : 0409
	DriverDesc : Media Control Devices
	DriverDesc : RAGE XL PCI
	Identifier : x86 Family 15 Model 4 Stepping 3
Run	ATIPTA : atiptaxx.exe
Run	FRISK FP-Scheduler: C:\Program Files\FSI\F-Prot\F-Sched.exe STARTUP
Run	F-StopW : C:\Program Files\FSI\F-Prot\F-StopW.EXE
Run	Intel Server Manager: C:\program files\intel\ServerManager\Server\bin\usm.exe
Run	ISUSPM : "C:\Program Files\Common Files\InstallShield\UpdateService\ISUSPM.exe" -scheduler
Run	MsmqIntCert : regsvr32 /s mqrt.dll
Run	PRONoMgrWired : C:\Program Files\Intel\PROSet\Wired\NCS\PROSet\PRONoMgr.exe

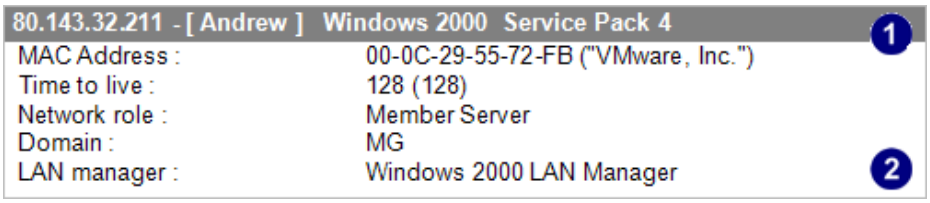
Screenshot 84 – Sample report showing system information

12	Installed application details for each host machine, including name, publisher and version
13	List showing password policy details security audit policy details
14	List of registry entry details for each host machine

Use this report to:

- List detailed technical information for each host machine, including services, installed applications, policies and devices.

8.2.4 Computer properties


80.143.32.211 - [Andrew] Windows 2000 Service Pack 4
MAC Address : 00-0C-29-55-72-FB ("VMware, Inc.")
Time to live : 128 (128)
Network role : Member Server
Domain : MG
LAN manager : Windows 2000 LAN Manager
1
2

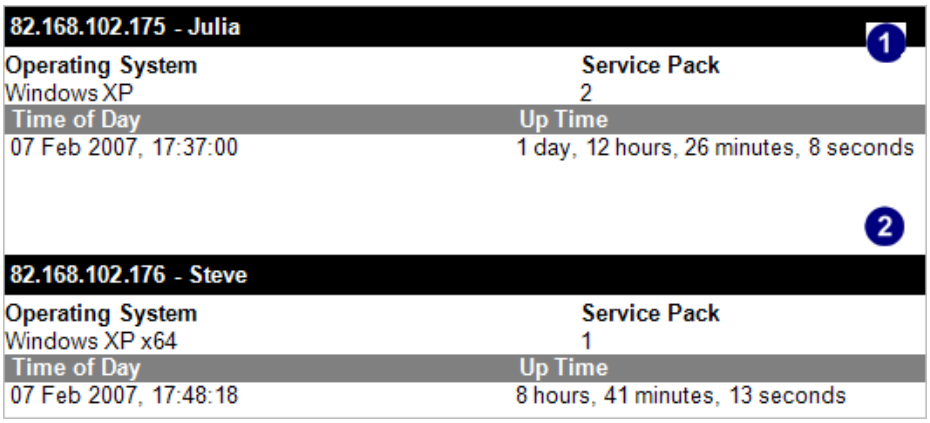
Screenshot 85 – Sample report showing computer properties

1	Host machine IP and name
2	Host machine details, including MAC address and domain

Use this report to:

- List information for each host machine, including MAC address, network role and domain.

8.2.5 Uptimes



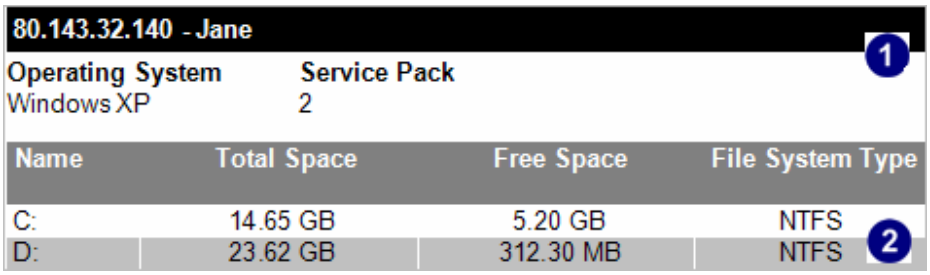
Screenshot 86 – Sample report showing uptimes

1	Host machine IP and name
2	Uptime details for each host machine, including time of day and uptime value

Use this report to:

- List uptime for each host machine, grouped by network scan.

8.2.6 Disk utilization



Screenshot 87 – Sample report showing disk utilization

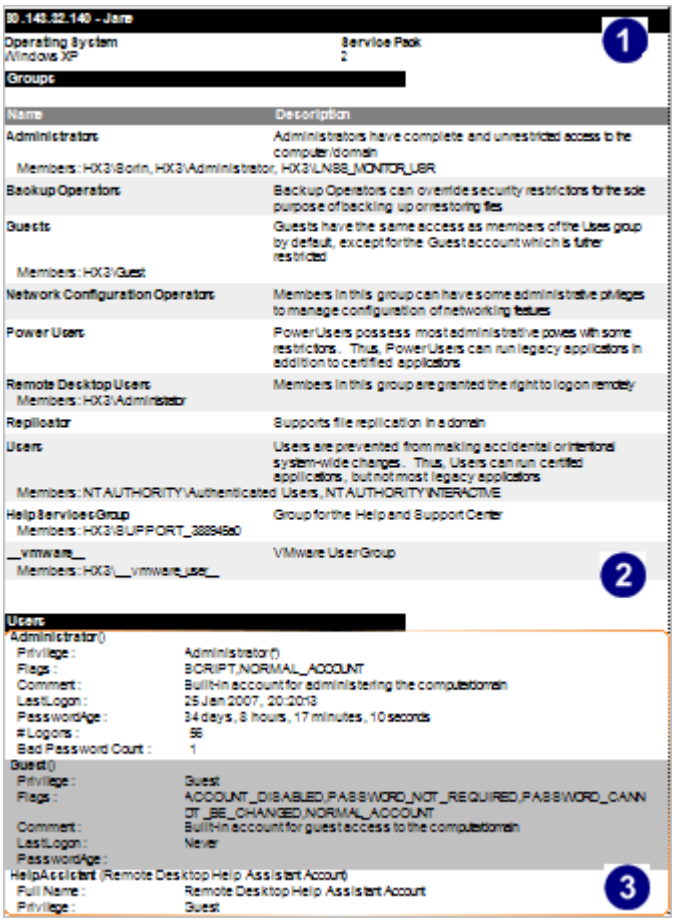
1	Host machine IP and name

2	Disk utilization details for each host machine, including drive name, file system type, total storage space and free storage space

Use this report to:

- List disk utilization information for each host machine, including file system type, total space and free space.

8.2.7 Groups and users



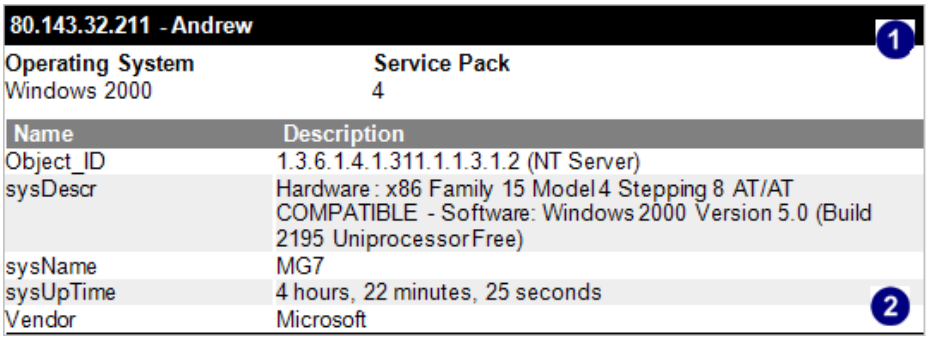
Screenshot 88 – Sample report showing groups and users

1	Host machine IP and name
2	List showing group details for each host machine, including name, description and members
3	List of user details for each group, including user name, privilege, last logon and bad password count

Use this report to:

- List group and user information for each host machine.

8.2.8 SNMP information



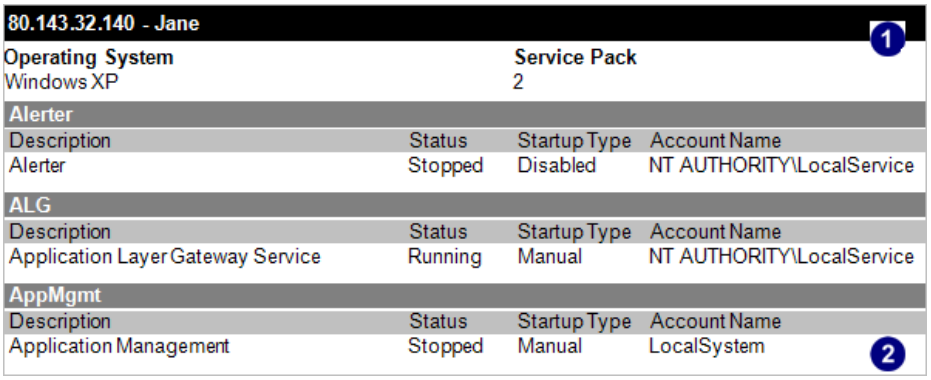
Screenshot 89 – Sample report showing SNMP information

1	Host machine IP and name
2	SNMP details for each host machine, including name and description

Use this report to:

- List SNMP information for each host machine, including name, description and uptime.

8.2.9 Services



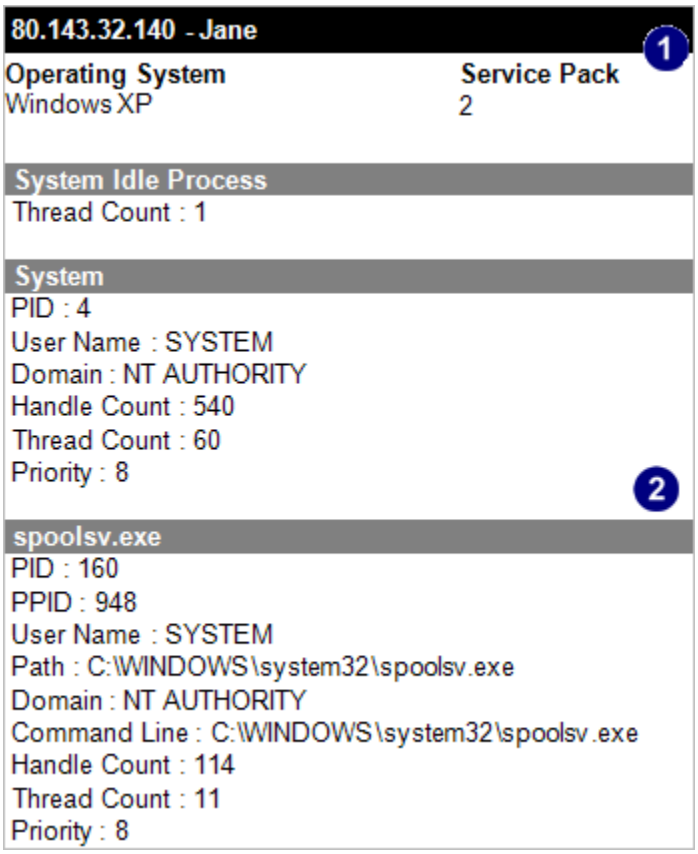
Screenshot 90 – Sample report showing services

1	Host machine IP and name
2	Service details for each host machine, including name, description, status, startup type and account name

Use this report to:

- List service information for each host machine, including description, status, and startup type and account name.

8.2.10 Processes



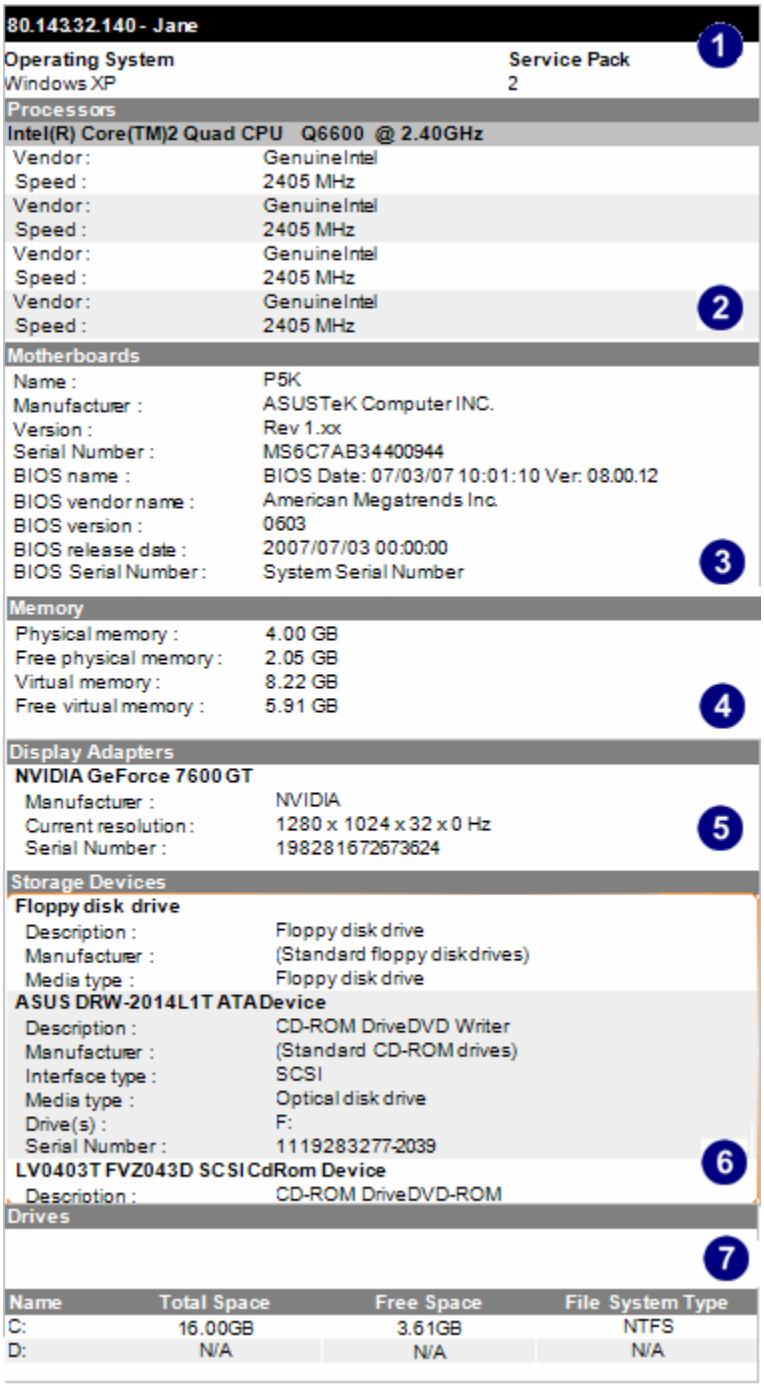
Screenshot 91 – Sample report showing processes

1	Host machine IP and name
2	Process details for each host machine, including process ID and account name

Use this report to:

- List process properties for each host machine.

8.2.11 Hardware Audit



80.143.32.140 - Jane (1)

Operating System	Service Pack
Windows XP	2

Processors

Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GHz

Vendor:	GenuineIntel
Speed :	2405 MHz
Vendor:	GenuineIntel
Speed :	2405 MHz
Vendor:	GenuineIntel
Speed :	2405 MHz
Vendor:	GenuineIntel
Speed :	2405 MHz

(2)

Motherboards

Name :	P5K
Manufacturer :	ASUSTeK Computer INC.
Version :	Rev 1.xx
Serial Number :	MS6C7AB34400944
BIOS name :	BIOS Date: 07/03/07 10:01:10 Ver: 08.00.12
BIOS vendor name :	American Megatrends Inc.
BIOS version :	0603
BIOS release date :	2007/07/03 00:00:00
BIOS Serial Number :	System Serial Number

(3)

Memory

Physical memory :	4.00 GB
Free physical memory :	2.05 GB
Virtual memory :	8.22 GB
Free virtual memory :	5.91 GB

(4)

Display Adapters

NVIDIA GeForce 7600 GT

Manufacturer :	NVIDIA
Current resolution :	1280 x 1024 x 32 x 0 Hz
Serial Number :	198281672673624

(5)

Storage Devices

Floppy disk drive

Description :	Floppy disk drive
Manufacturer :	(Standard floppy disk drives)
Media type :	Floppy disk drive

ASUS DRW-2014L1T ATA Device

Description :	CD-ROM Drive\DVD Writer
Manufacturer :	(Standard CD-ROM drives)
Interface type :	SCSI
Media type :	Optical disk drive
Drive(s) :	F:
Serial Number :	1119283277-2039

LV0403T FVZ043D SCSI CdRom Device

Description :	CD-ROM Drive\DVD-ROM

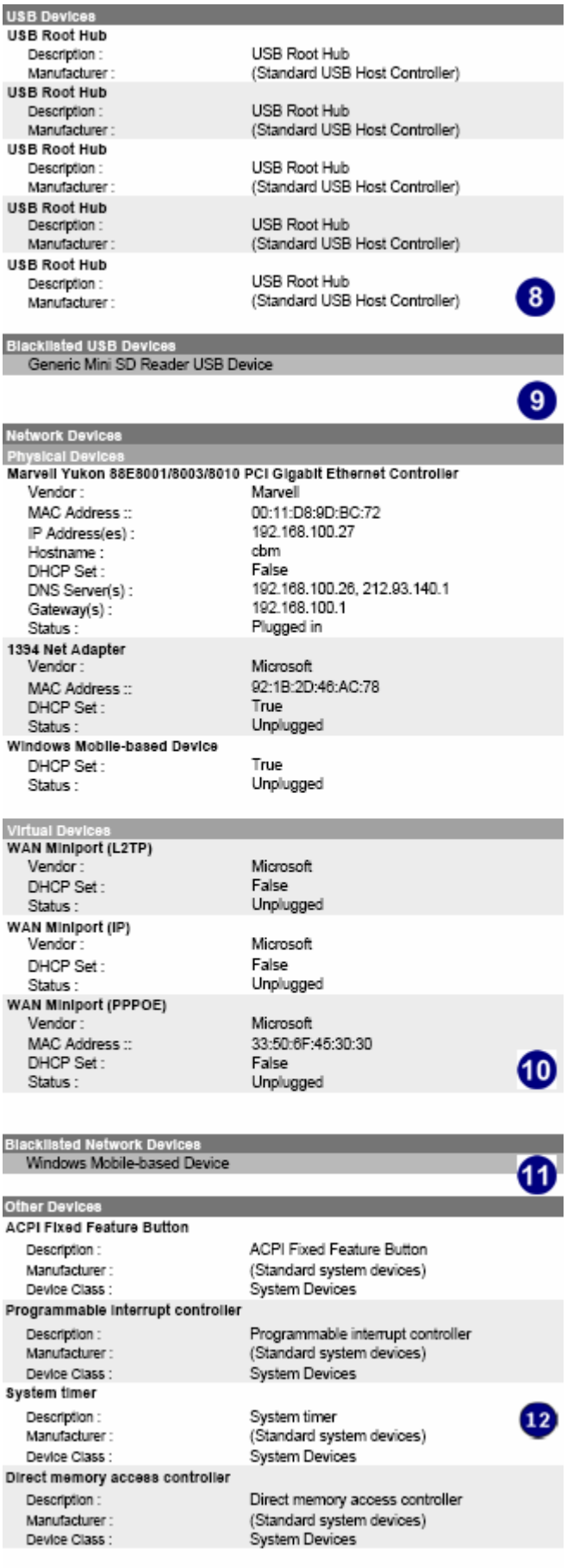
(6)

Drives

(7)

Name	Total Space	Free Space	File System Type
C:	16.00GB	3.61GB	NTFS
D:	N/A	N/A	N/A

Screenshot 92 - Sample report showing hardware audit - part 1 of 2



USB Devices

USB Root Hub
Description : USB Root Hub
Manufacturer : (Standard USB Host Controller)

USB Root Hub
Description : USB Root Hub
Manufacturer : (Standard USB Host Controller)

USB Root Hub
Description : USB Root Hub
Manufacturer : (Standard USB Host Controller)

USB Root Hub
Description : USB Root Hub
Manufacturer : (Standard USB Host Controller)

USB Root Hub
Description : USB Root Hub
Manufacturer : (Standard USB Host Controller)

8

Blacklisted USB Devices
Generic Mini SD Reader USB Device

9

Network Devices

Physical Devices

Marvell Yukon 88E8001/8003/8010 PCI Gigabit Ethernet Controller
Vendor : Marvell
MAC Address :: 00:11:D8:9D:BC:72
IP Address(es) : 192.168.100.27
Hostname : cbm
DHCP Set : False
DNS Server(s) : 192.168.100.26, 212.93.140.1
Gateway(s) : 192.168.100.1
Status : Plugged in

1394 Net Adapter
Vendor : Microsoft
MAC Address :: 92:1B:2D:46:AC:78
DHCP Set : True
Status : Unplugged

Windows Mobile-based Device
DHCP Set : True
Status : Unplugged

Virtual Devices

WAN Miniport (L2TP)
Vendor : Microsoft
DHCP Set : False
Status : Unplugged

WAN Miniport (IP)
Vendor : Microsoft
DHCP Set : False
Status : Unplugged

WAN Miniport (PPPOE)
Vendor : Microsoft
MAC Address :: 33:50:6F:45:30:30
DHCP Set : False
Status : Unplugged

10

Blacklisted Network Devices
Windows Mobile-based Device

11

Other Devices

ACPI Fixed Feature Button
Description : ACPI Fixed Feature Button
Manufacturer : (Standard system devices)
Device Class : System Devices

Programmable interrupt controller
Description : Programmable interrupt controller
Manufacturer : (Standard system devices)
Device Class : System Devices

System timer
Description : System timer
Manufacturer : (Standard system devices)
Device Class : System Devices

12

Direct memory access controller
Description : Direct memory access controller
Manufacturer : (Standard system devices)
Device Class : System Devices

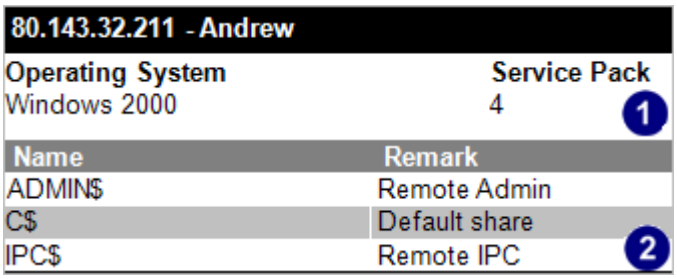
Screenshot 93 - Sample report showing hardware audit - part 2 of 2

1	Host machine IP and name
2	Processor information
3	Motherboard information
4	Physical and virtual memory
5	Display adaptors
6	Storage devices
7	Drive name, space allocation and file system type
8	USB device information
9	Blacklisted USB devices
10	Physical and virtual network devices
11	Blacklisted network devices
12	Other devices

Use this report to identify all devices detected on the network for scan computers

NOTE: Devices are grouped by categories. Categories with no devices detected are not displayed.

8.2.12 Shares



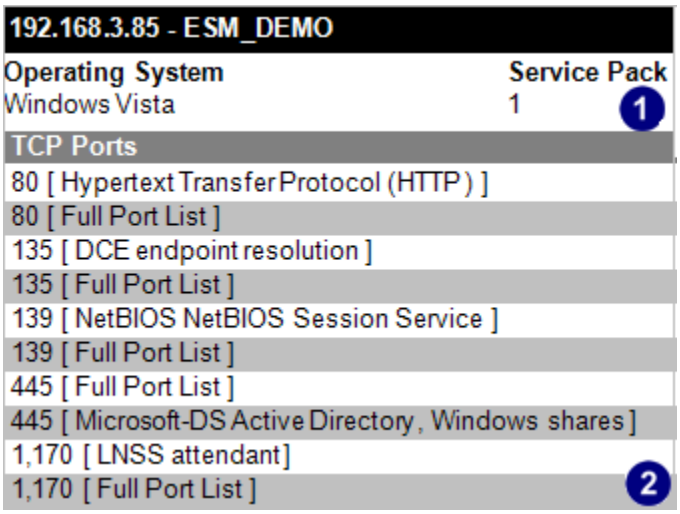
Screenshot 94 – Sample report showing shares

1	Host machine IP and name
2	Share folder details for each host machine, including name and remarks

Use this report to:

- List information on shared folders for each host machine.

8.2.13 Open ports


192.168.3.85 - ESM_DEMO
Operating System
Service Pack
Windows Vista
1
1
TCP Ports
80 [Hypertext Transfer Protocol (HTTP)]
80 [Full Port List]
135 [DCE endpoint resolution]
135 [Full Port List]
139 [NetBIOS NetBIOS Session Service]
139 [Full Port List]
445 [Full Port List]
445 [Microsoft-DS Active Directory, Windows shares]
1,170 [LNSS attendant]
1,170 [Full Port List]
2

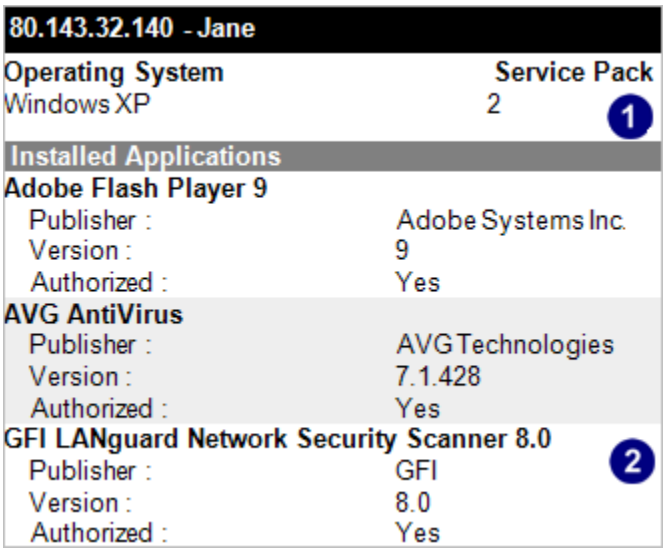
Screenshot 95 – Sample report showing open ports

1	Host machine IP and name
2	Open port details for each host machine, including port number and name

Use this report to:

- List open ports detected for each host on the network including port number and name.

8.2.14 Installed applications by Host



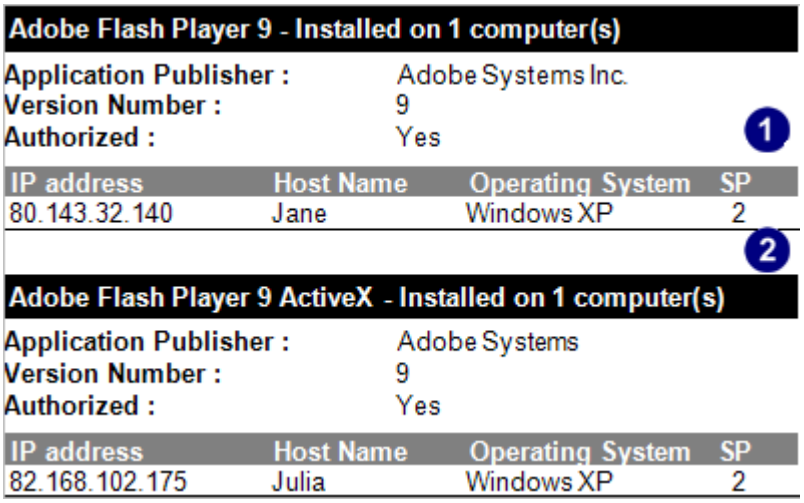
Screenshot 96 – Sample report showing installed applications

1	Host machine IP and name
2	Installed application details for each host machine, including name, publisher and version

Use this report to:

- List installed applications detected for each network host scanned, including publisher and version details.

8.2.15 Application Inventory


Adobe Flash Player 9 - Installed on 1 computer(s)
Application Publisher : Adobe Systems Inc.
Version Number : 9
Authorized : Yes
1
IP address Host Name Operating System SP
80.143.32.140 Jane Windows XP 2
2
Adobe Flash Player 9 ActiveX - Installed on 1 computer(s)
Application Publisher : Adobe Systems
Version Number : 9
Authorized : Yes
IP address Host Name Operating System SP
82.168.102.175 Julia Windows XP 2

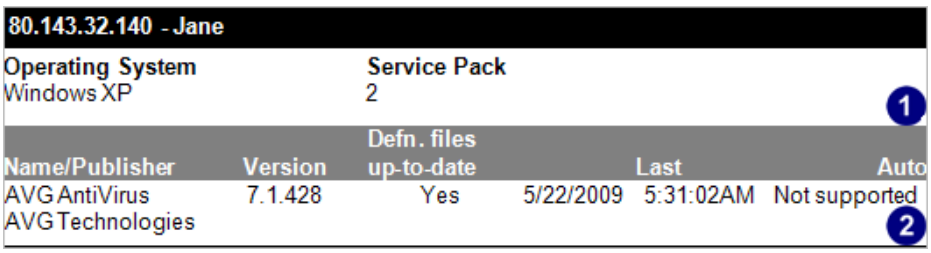
Screenshot 97 - Sample report showing applications inventory

1	Installed application name and details
2	List of computers having application installed

Use this report to:

- Identify all computers which have specific software installed on them.

8.2.16 Antivirus Applications



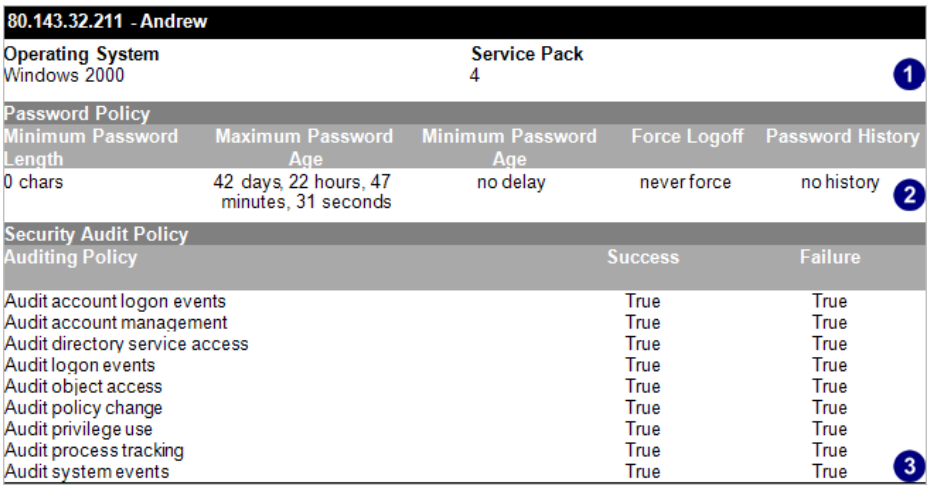
Screenshot 98 – Sample report showing installed anti-virus applications

1	Host machine IP and name
2	Antivirus application details for each host machine, including name, publisher and version

Use this report to:

- List installed antivirus applications detected for each network host scanned, including publisher and version details.

8.2.17 Auditing Policies



80.143.32.211 - Andrew

Operating System	Service Pack
Windows 2000	4

Password Policy

Minimum Password Length	Maximum Password Age	Minimum Password Age	Force Logoff	Password History
0 chars	42 days, 22 hours, 47 minutes, 31 seconds	no delay	never force	no history

Security Audit Policy

Auditing Policy	Success	Failure
Audit account logon events	True	True
Audit account management	True	True
Audit directory service access	True	True
Audit logon events	True	True
Audit object access	True	True
Audit policy change	True	True
Audit privilege use	True	True
Audit process tracking	True	True
Audit system events	True	True

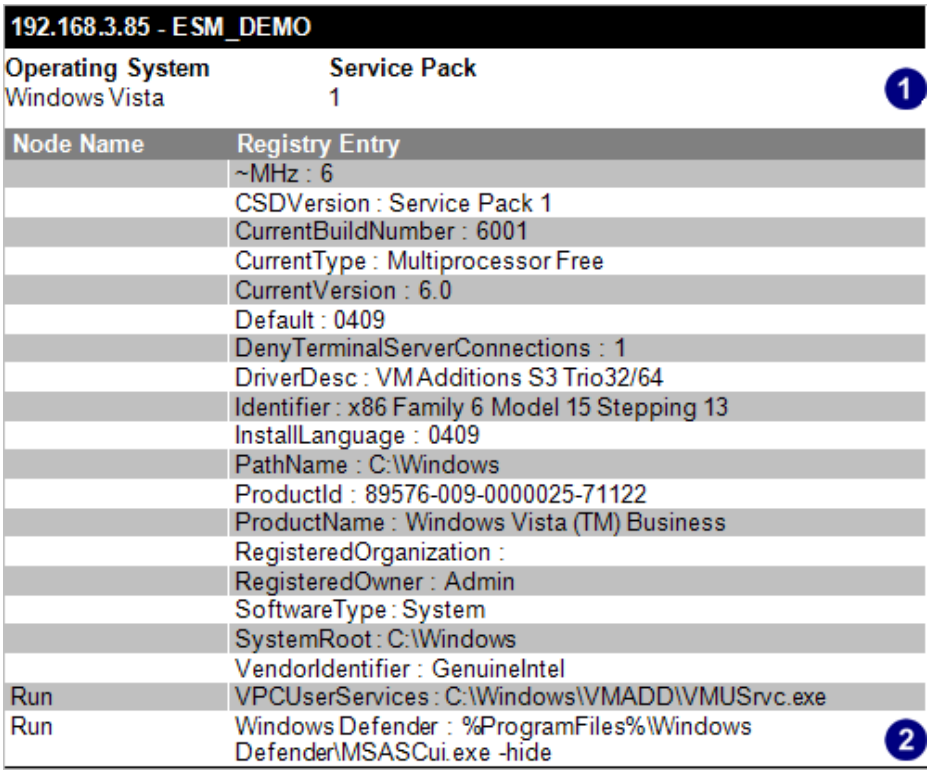
Screenshot 99 – Sample report showing policies

1	Host machine IP and name
2	Password policy details for each host machine, including minimum password length and password history
3	List showing security audit policy details for each host machine

Use this report to:

- List password and security audit policy settings for each network host scanned.

8.2.18 Registry information



192.168.3.85 - ESM_DEMO

Operating System	Service Pack
Windows Vista	1

Node Name	Registry Entry
	~MHz : 6
	CSDVersion : Service Pack 1
	CurrentBuildNumber : 6001
	CurrentType : Multiprocessor Free
	CurrentVersion : 6.0
	Default : 0409
	DenyTerminalServerConnections : 1
	DriverDesc : VM Additions S3 Trio32/64
	Identifier : x86 Family 6 Model 15 Stepping 13
	InstallLanguage : 0409
	PathName : C:\Windows
	ProductId : 89576-009-0000025-71122
	ProductName : Windows Vista (TM) Business
	RegisteredOrganization :
	RegisteredOwner : Admin
	SoftwareType : System
	SystemRoot : C:\Windows
	VendorIdentifier : GenuineIntel
Run	VPCUserServices : C:\Windows\VMADD\VMUSrvc.exe
Run	Windows Defender : %ProgramFiles%\Windows Defender\MSASCui.exe -hide

Screenshot 100 – Sample report showing registry information

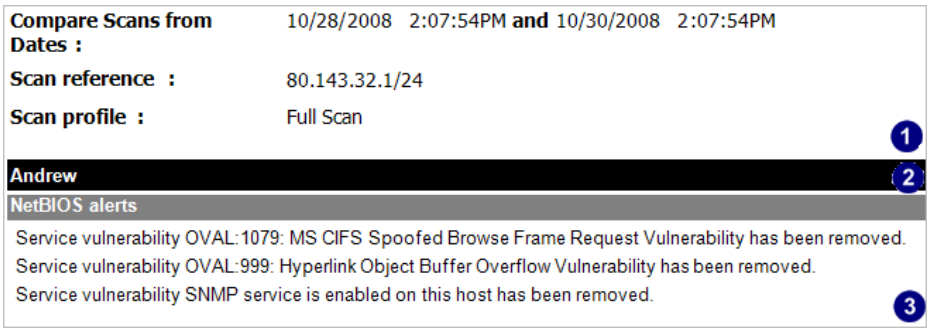
1	Host machine IP and name
2	List of registry entry details for each host machine

Use this report to:

- List system related registry information for each network host scanned.

8.3 Results comparison

8.3.1 Network security log by date


Compare Scans from Dates :
10/28/2008 2:07:54PM and 10/30/2008 2:07:54PM
Scan reference :
80.143.32.1/24
Scan profile :
Full Scan
1
Andrew
2
NetBIOS alerts
Service vulnerability OVAL:1079: MS CIFS Spoofed Browse Frame Request Vulnerability has been removed.
Service vulnerability OVAL:999: Hyperlink Object Buffer Overflow Vulnerability has been removed.
Service vulnerability SNMP service is enabled on this host has been removed.
3

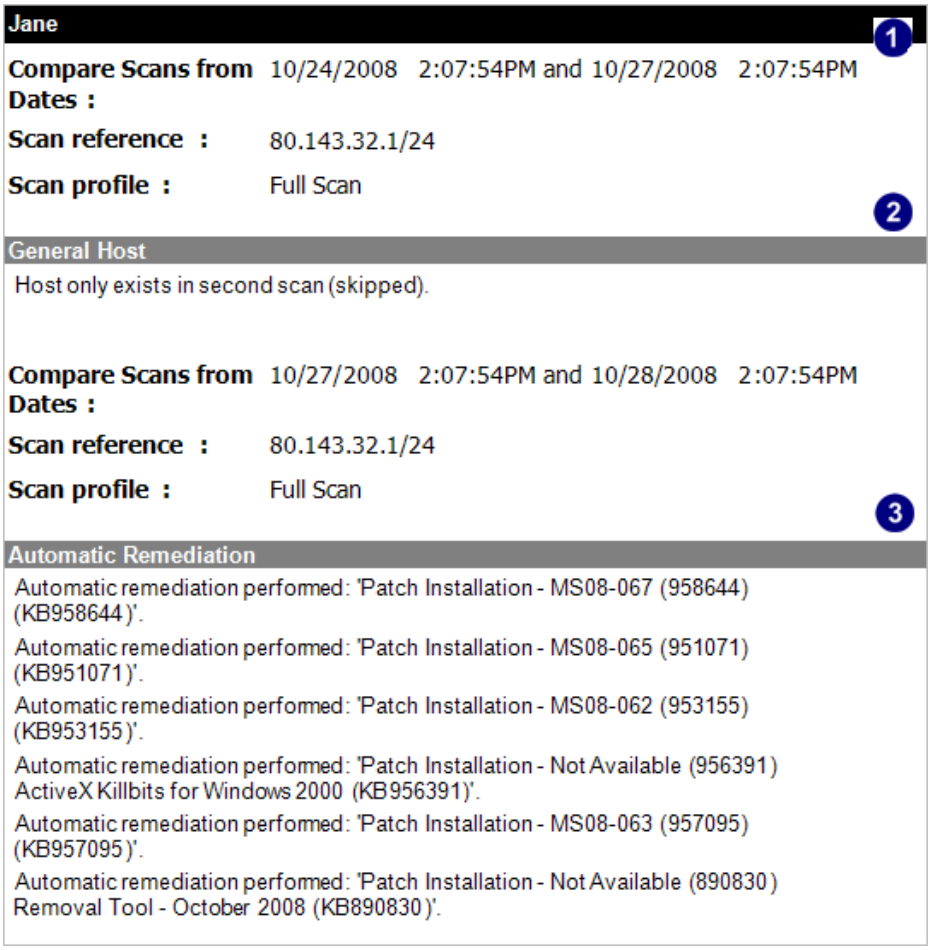
Screenshot 101 – Sample report showing network security log by date

1	Network security scans to be compared
2	Host machine on which the comparison was made
3	List of differences found between comparisons for each host machine. Differences are grouped by category, including backdoors, missing hot fixes, password policy, USB devices and applications

Use this report to:

- Compare results of consecutive scans that have a common profile and target, grouped by scan date.

8.3.2 Network security log by host


Jane
1
Compare Scans from Dates : 10/24/2008 2:07:54PM and 10/27/2008 2:07:54PM
Scan reference : 80.143.32.1/24
Scan profile : Full Scan
2
General Host
Host only exists in second scan (skipped).
Compare Scans from Dates : 10/27/2008 2:07:54PM and 10/28/2008 2:07:54PM
Scan reference : 80.143.32.1/24
Scan profile : Full Scan
3
Automatic Remediation
Automatic remediation performed: 'Patch Installation - MS08-067 (958644) (KB958644)'.
Automatic remediation performed: 'Patch Installation - MS08-065 (951071) (KB951071)'.
Automatic remediation performed: 'Patch Installation - MS08-062 (953155) (KB953155)'.
Automatic remediation performed: 'Patch Installation - Not Available (956391) ActiveX Killbits for Windows 2000 (KB956391)'.
Automatic remediation performed: 'Patch Installation - MS08-063 (957095) (KB957095)'.
Automatic remediation performed: 'Patch Installation - Not Available (890830) Removal Tool - October 2008 (KB890830)'.

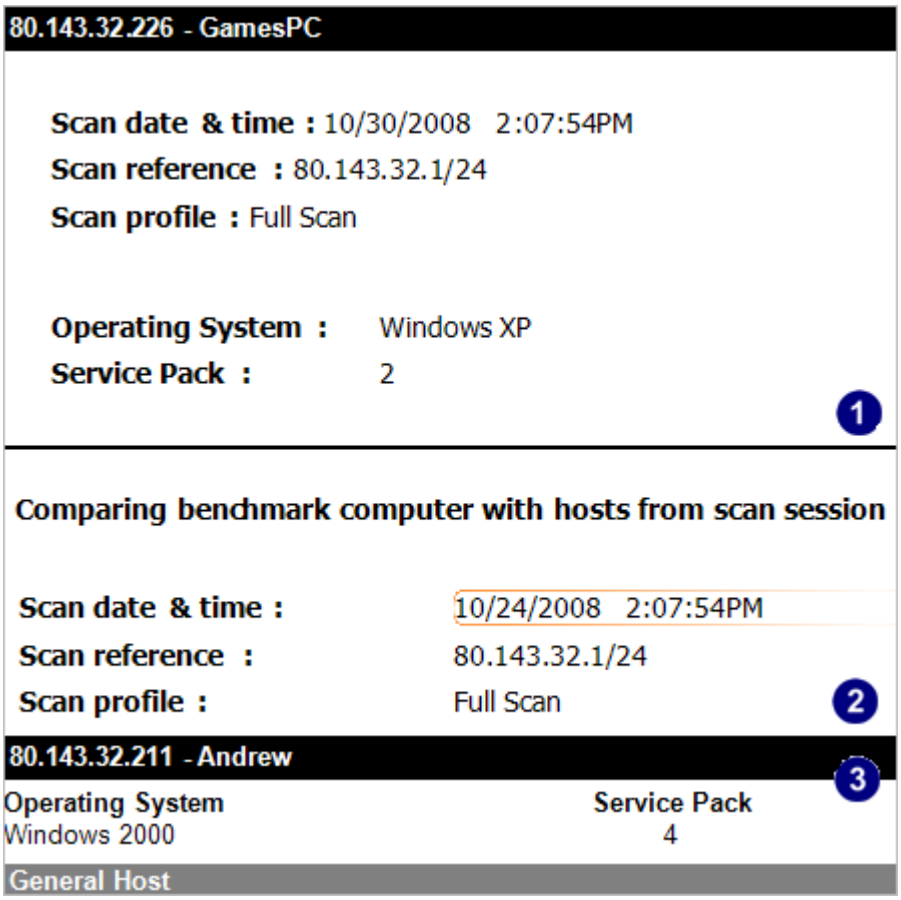
Screenshot 102 – Sample report showing network security log by host

1	Host machine on which the comparison was made
2	Network security scans which were compared
3	List of differences found between comparisons for each host machine. Differences are grouped by category, including backdoors, missing hot fixes, password policy, USB devices and applications

Use this report to:

- Compare results of consecutive scans that have a common profile and target, grouped by host machine.

8.3.3 Baseline changes comparison



Screenshot 103 – Sample report showing security settings comparison

1	Details of the computer used as comparison standard, including scan date, and scan profile
2	List showing host machines with which the standard computer was compared
3	List of differences found when comparing the host machines with the standard computer. Differences are grouped by category, including backdoors, missing hot fixes, password policy, USB devices and applications

Use this report to compare results between a chosen computer, used as benchmark, and host machines scanned with the same profile and having the same target.

9. Troubleshooting

9.1 Introduction

The troubleshooting chapter explains how you should go about resolving any software issues that you might encounter. The main sources of information available to users are:

- The manual – most issues can be solved by reading this manual.
- GFI Knowledge Base articles
- Web forum
- Contacting GFI Technical Support

9.2 Knowledge Base

GFI maintains a Knowledge Base, which includes answers to the most common problems. If you have a problem, please consult the Knowledge Base first. The Knowledge Base always has the most up-to-date listing of technical support questions and patches. To access the Knowledge Base, visit http://kbase.gfi.com/.

9.3 Web Forum

User to user technical support is available via the web forum. The forum can be found at: http://forums.gfi.com/.

9.4 Request technical support

If you have referred to this manual and our Knowledge Base articles, and you still cannot solve issues with the software, contact the GFI Technical Support team by filling in an online support request form or by phone.

- **Online**: Fill out the support request form on: http://support.gfi.com/supportrequestform.asp. Follow the instructions on this page closely to submit your support request.
- **Phone**: To obtain the correct technical support phone number for your region please visit: http://www.gfi.com/company/contact.htm.

NOTE: Before you contact our Technical Support team, please have your Customer ID available. Your Customer ID is the online account number that is assigned to you when you first register your license keys in our Customer Area at: http://customers.gfi.com.

We will answer your query within 24 hours or less, depending on your time zone.

9.5 Build notifications

We strongly suggest that you subscribe to our build notifications list. This way, you will be immediately notified about new product builds. To subscribe to our build notifications, visit: http://www.gfi.com/pages/productmailing.htm.

Index

C

configuration settings 42
custom reports 3, 5, 15, 24, 25

D

data filters 5, 15
database source 40, 41, 42
default reports 3, 9, 14
distribution of reports 4

E

export reports 5

F

favorite reports 3, 14, 24
filter conditions 17
framework 1, 2, 3, 4, 7

I

installation 5, 7, 8, 39

L

license 31

N

navigation button 3, 9, 10, 11, 14, 15, 21, 23, 24, 27, 28, 30, 31, 32, 33, 35, 36, 39, 40, 41, 48, 49

P

product ReportPack 3
Product Selection drop down list 8, 48

R

Report scheduling 2, 4

S

schedule activity monitor 31
scheduled reports 3, 5, 30, 32
security scan 18
System requirements 7

T

Troubleshooting 85

U

user interface 3, 30, 31, 39

W

wizard 7, 33